Security on the Line: Modern Curve-based Cryptography

Joost Renes

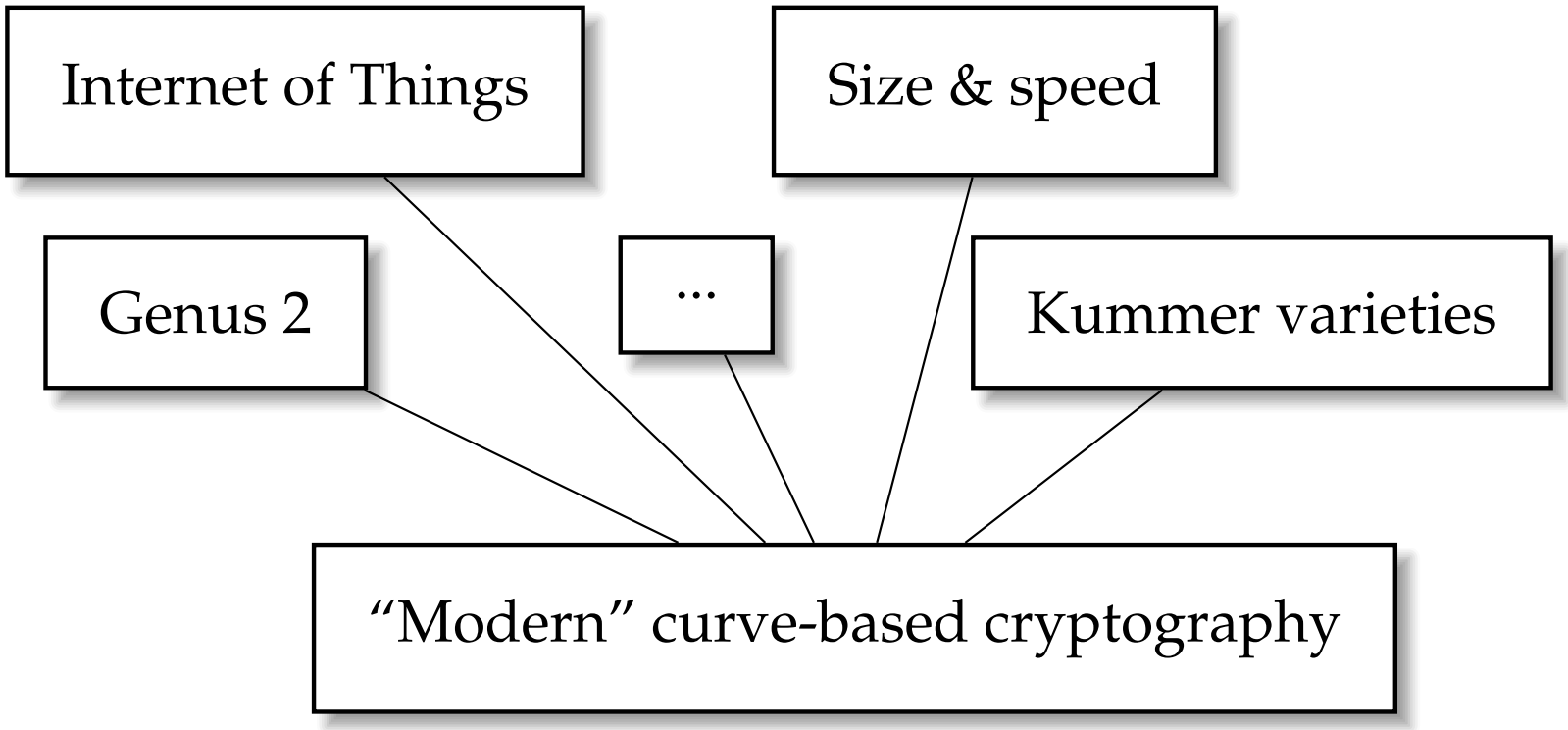
SCA Workshop

18 June 2019

Modern curve-based cryptography

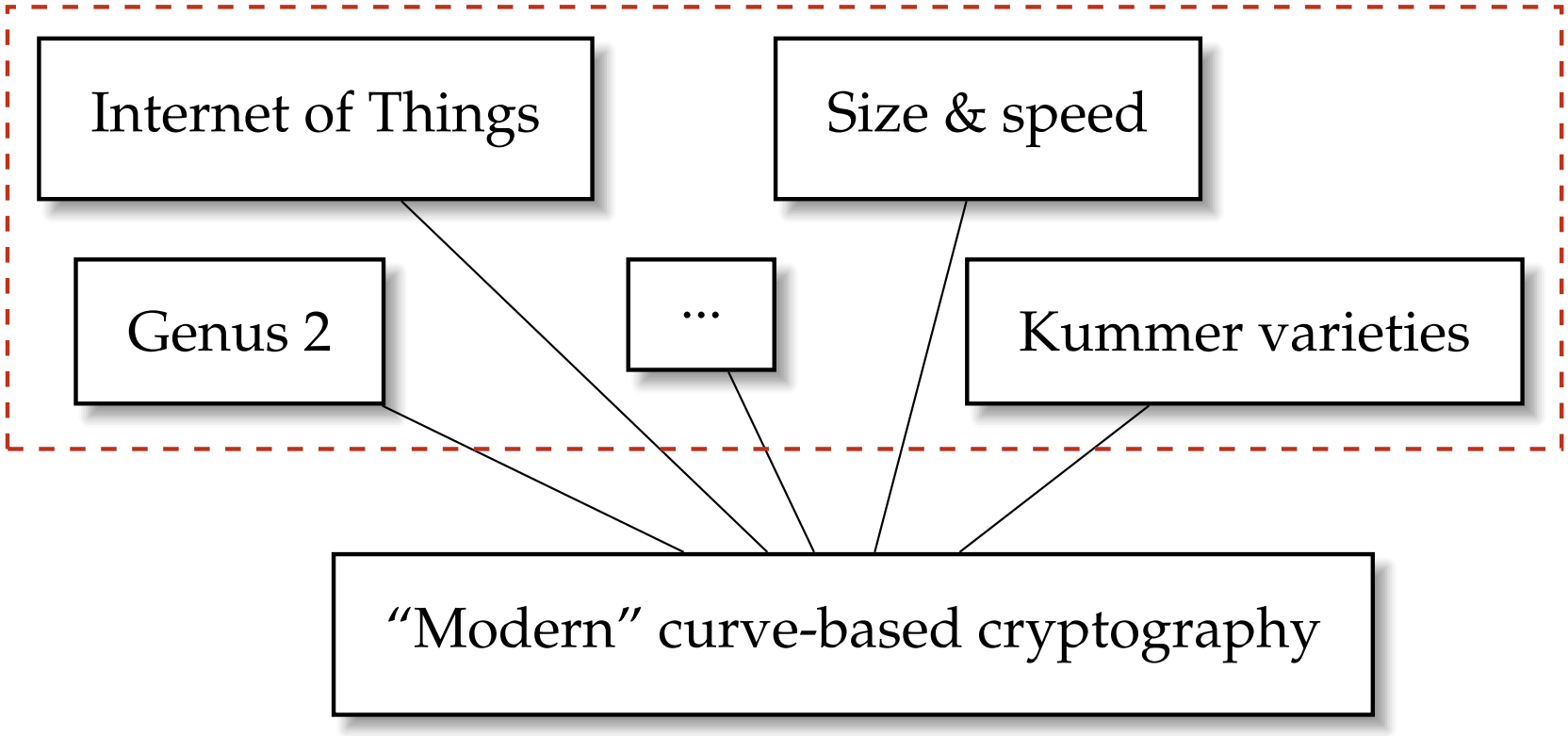
"Modern" curve-based cryptography

Modern curve-based cryptography

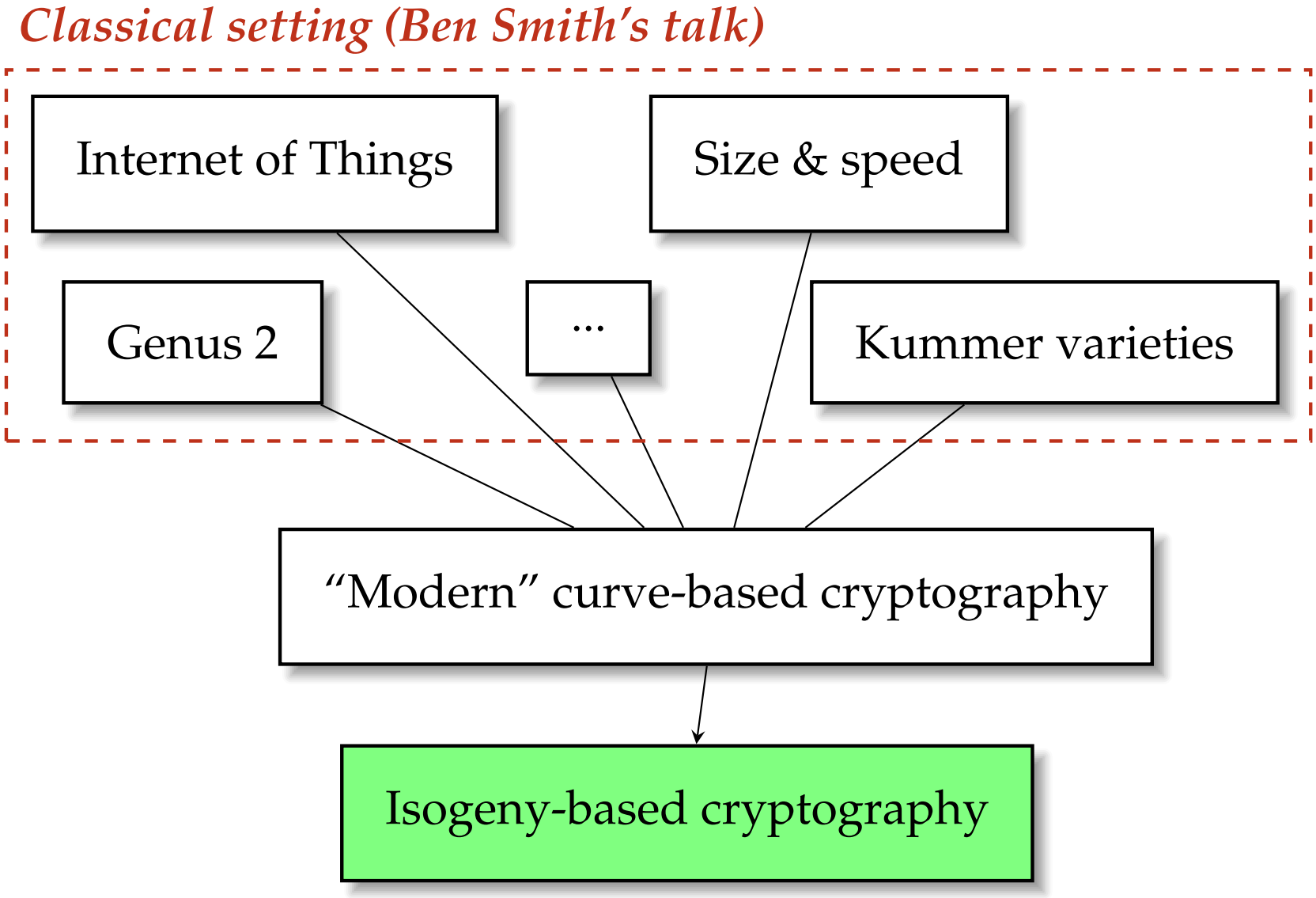


Modern curve-based cryptography

Classical setting (Ben Smith's talk)



Modern curve-based cryptography



Elliptic curves in cryptography

Discrete-log-based elliptic-curve cryptography [Mil86; Kob87]

Elliptic curves in cryptography

Discrete-log-based elliptic-curve cryptography [Mil86; Kob87]

Ordinary isogeny-based group actions [Cou06; RS06; DKS18]

Elliptic curves in cryptography

Discrete-log-based elliptic-curve cryptography [Mil86; Kob87]

Ordinary isogeny-based group actions [Cou06; RS06; DKS18]

Supersingular isogeny-based cryptography / $\mathbb{F}_{p^2}$ [CLG09; JF11]

Elliptic curves in cryptography

Discrete-log-based elliptic-curve cryptography [Mil86; Kob87]

Ordinary isogeny-based group actions [Cou06; RS06; DKS18]

Supersingular isogeny-based cryptography / $\mathbb{F}_{p^2}$ [CLG09; JF11]

Supersingular isogeny-based group actions / $\mathbb{F}_p$ [Cas+18]

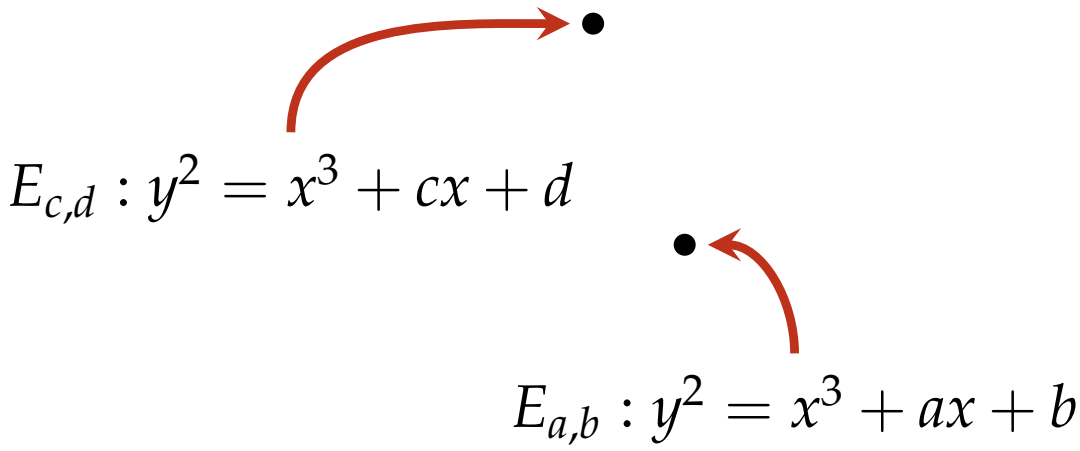
Elliptic curves & isogenies (1)

Fixed: prime p

$$E_{a,b} : y^2 = x^3 + ax + b$$

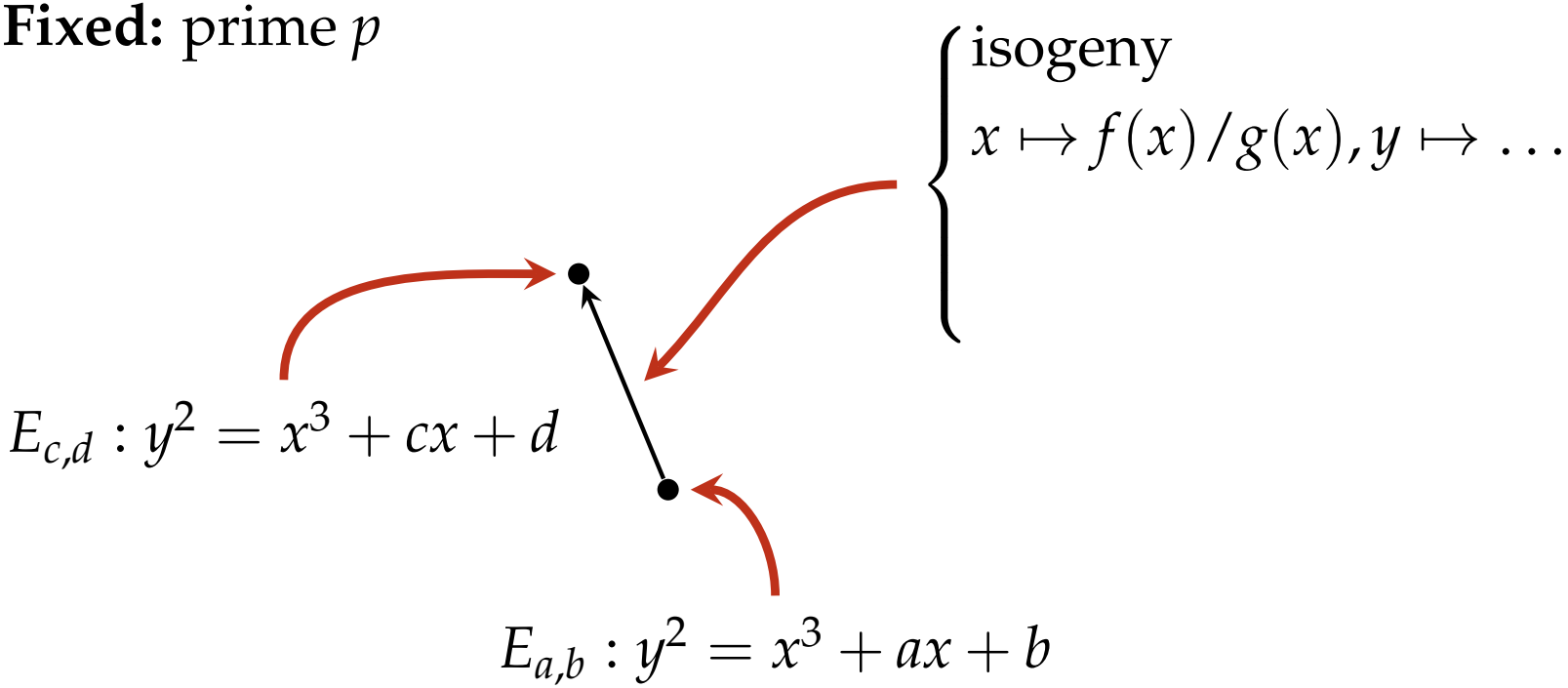
Elliptic curves & isogenies (1)

Fixed: prime p



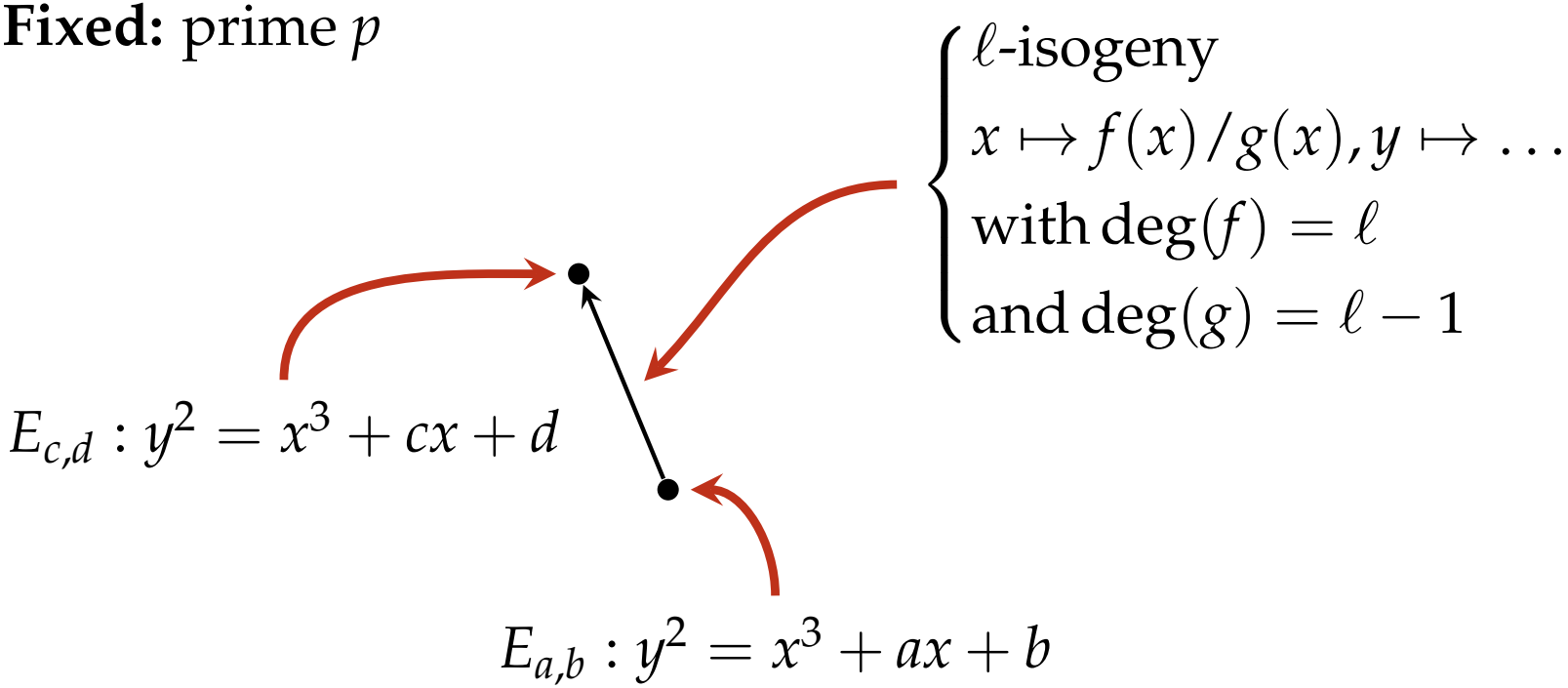
Elliptic curves & isogenies (1)

Fixed: prime p



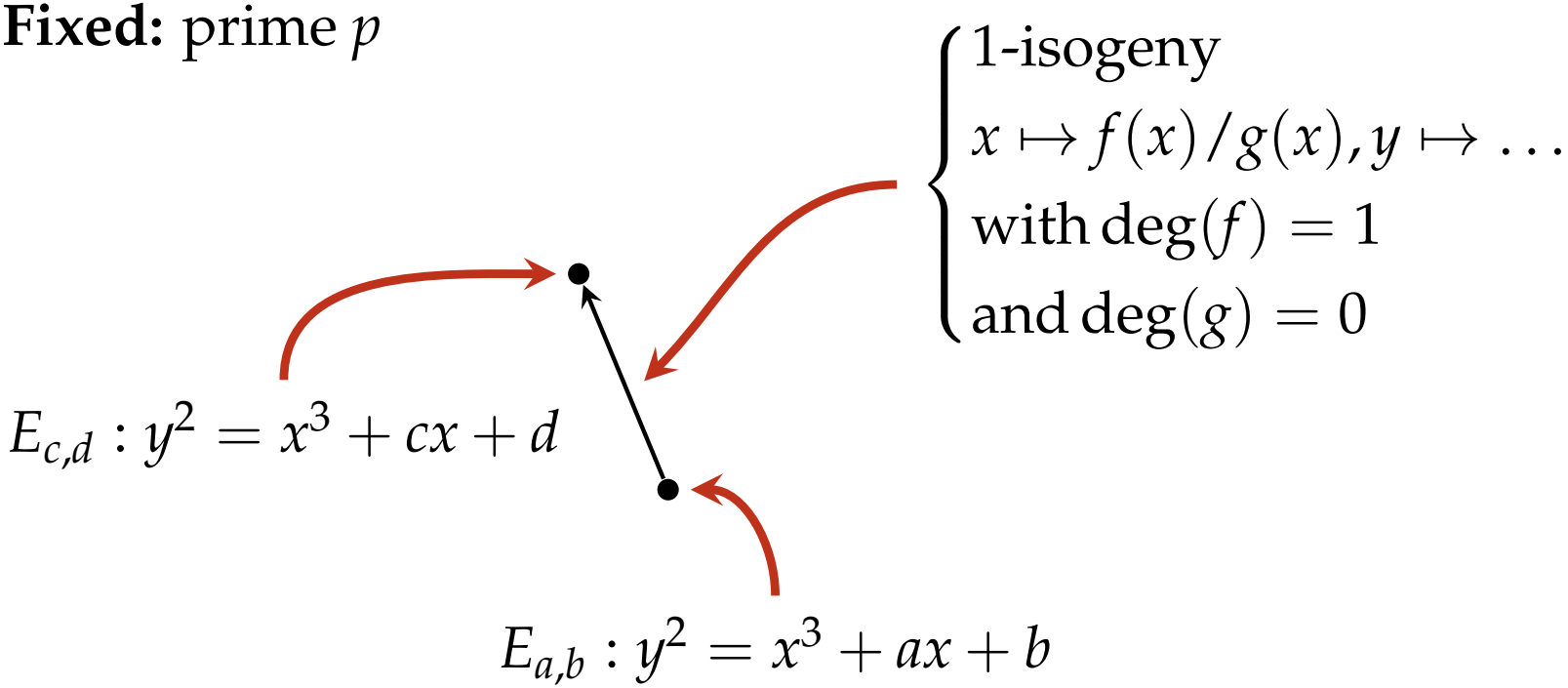
Elliptic curves & isogenies (1)

Fixed: prime p



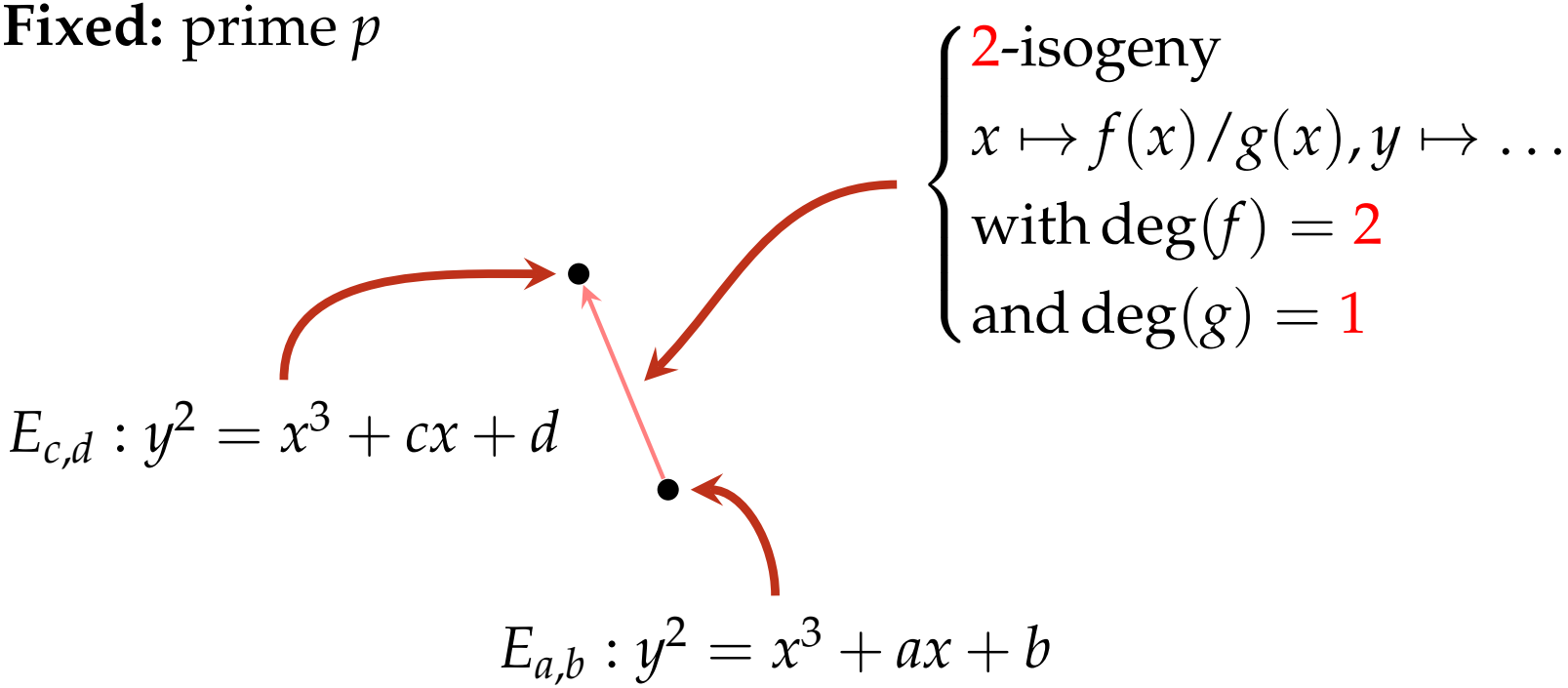
Elliptic curves & isogenies (1)

Fixed: prime p



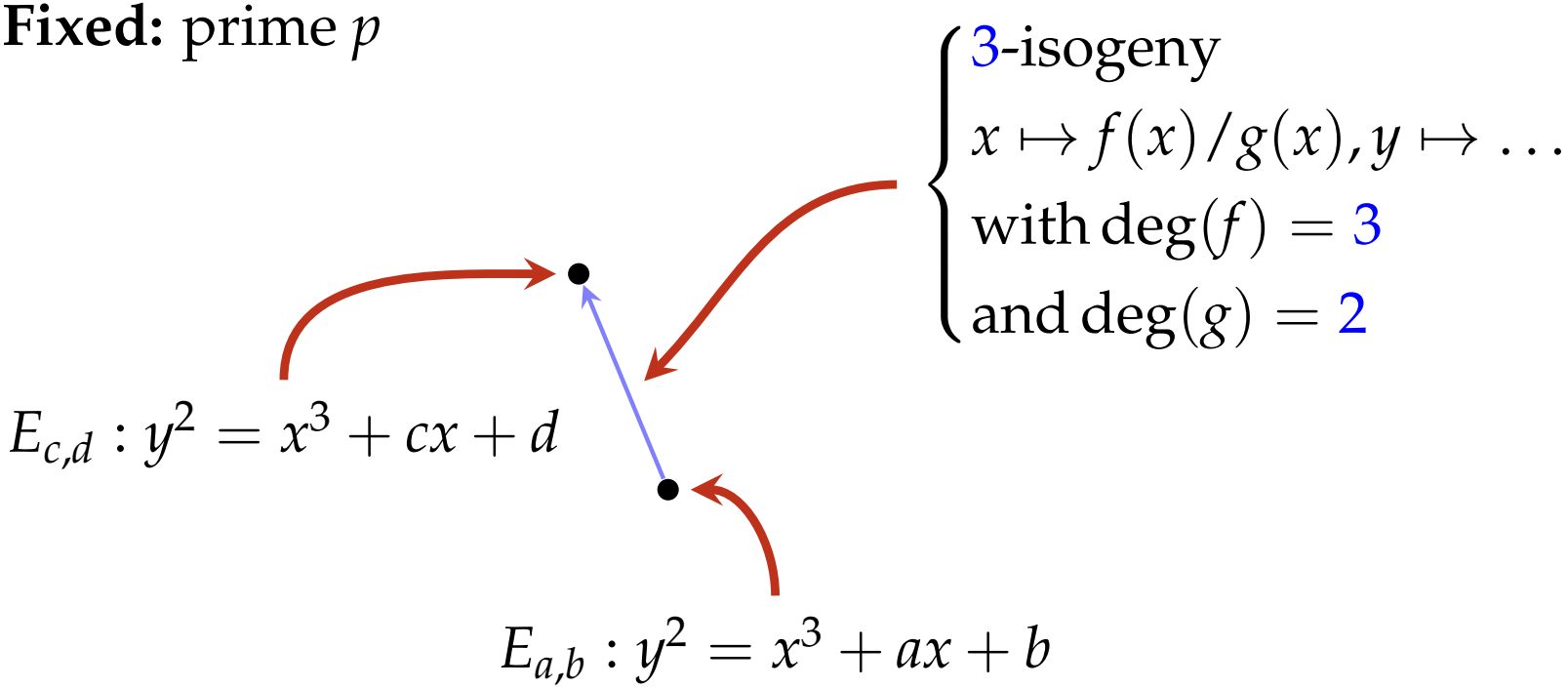
Elliptic curves & isogenies (1)

Fixed: prime p



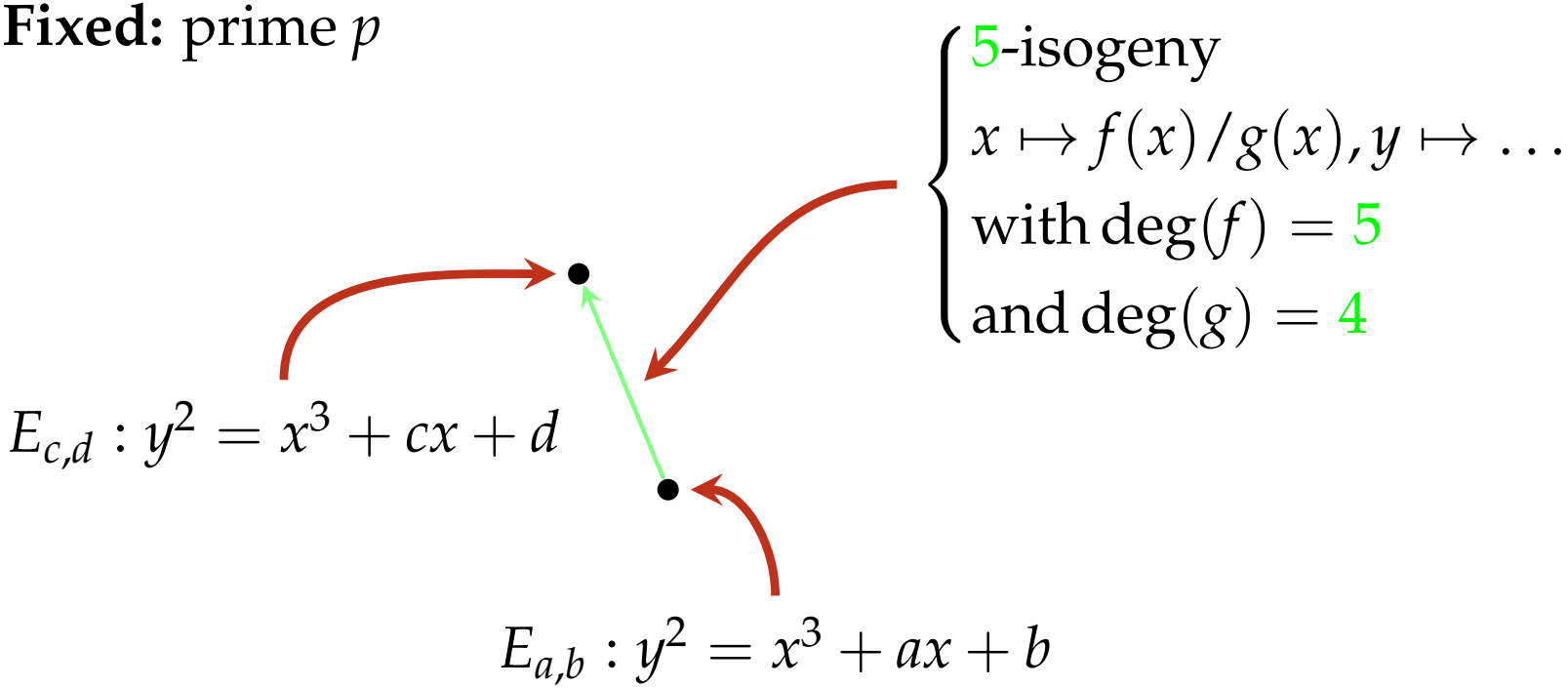
Elliptic curves & isogenies (1)

Fixed: prime p



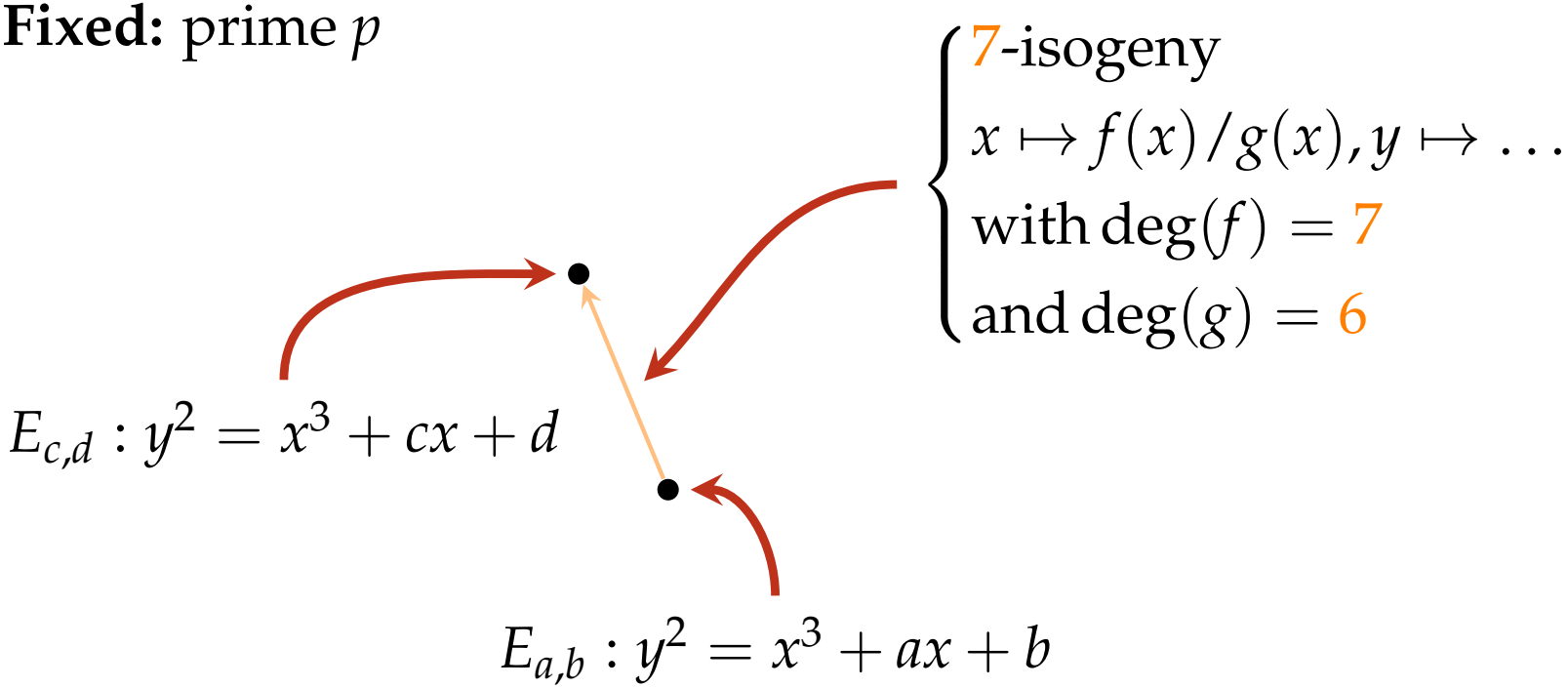
Elliptic curves & isogenies (1)

Fixed: prime p



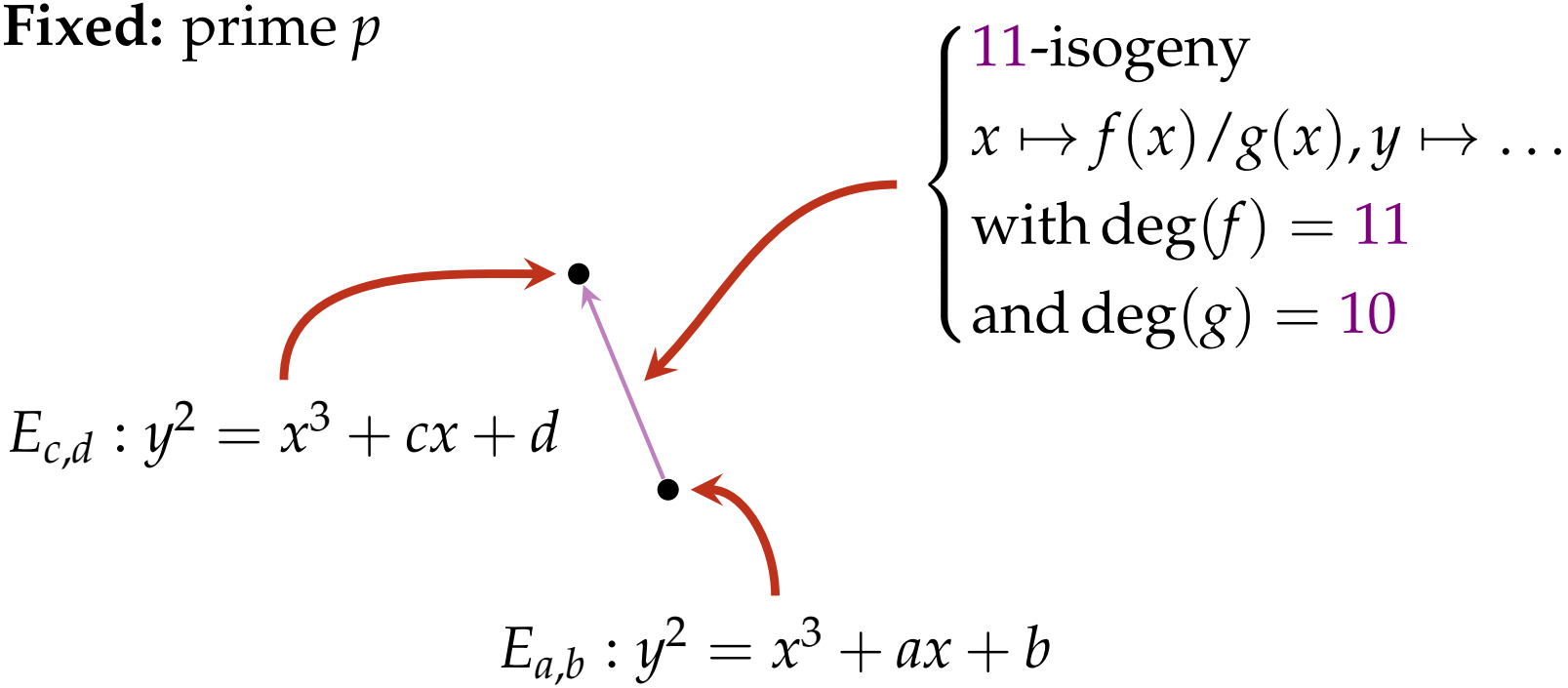
Elliptic curves & isogenies (1)

Fixed: prime p



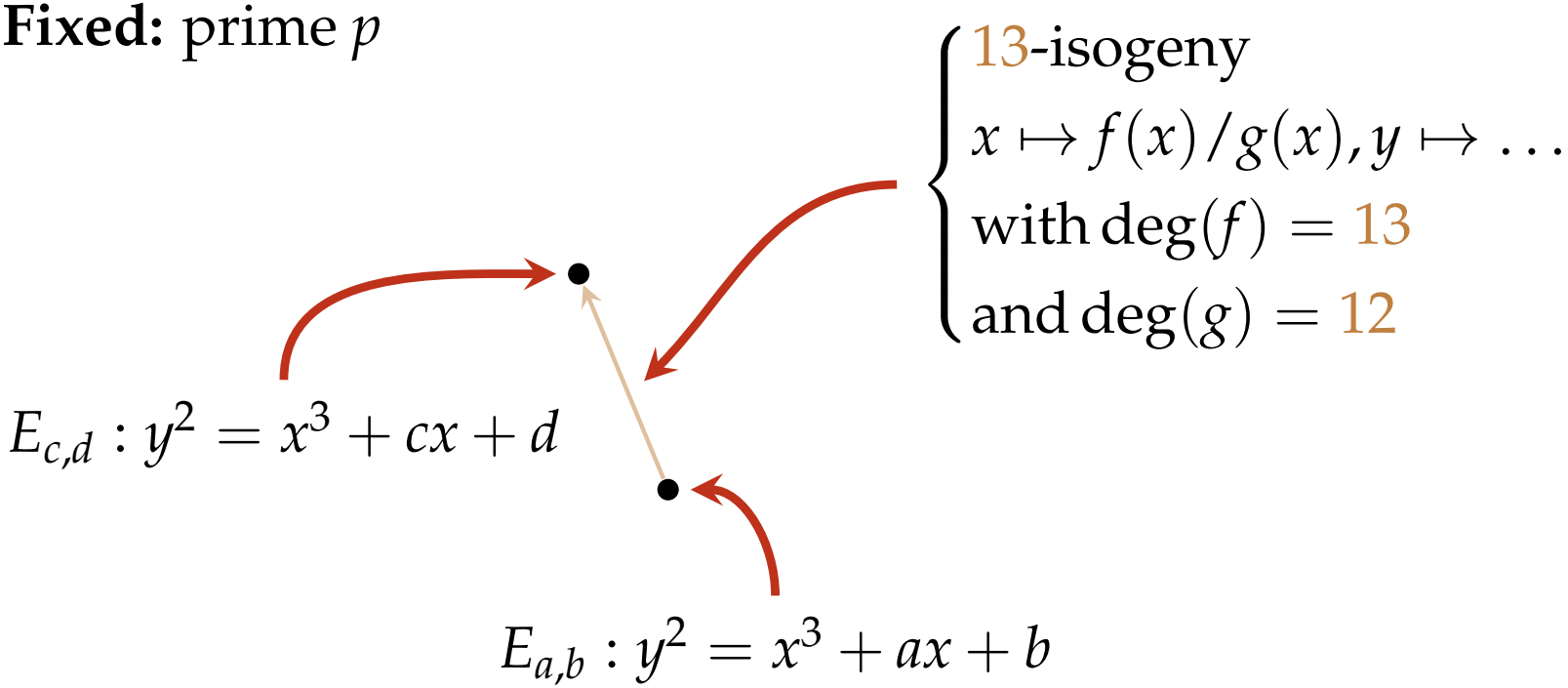
Elliptic curves & isogenies (1)

Fixed: prime p



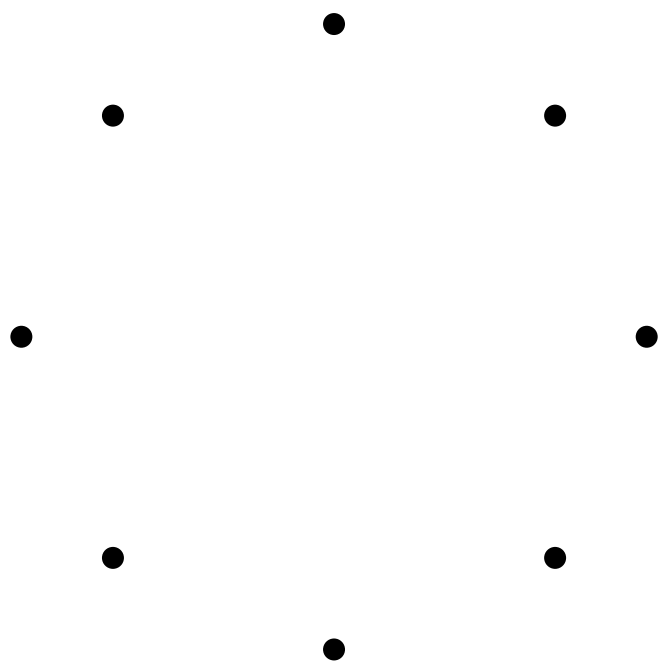
Elliptic curves & isogenies (1)

Fixed: prime p



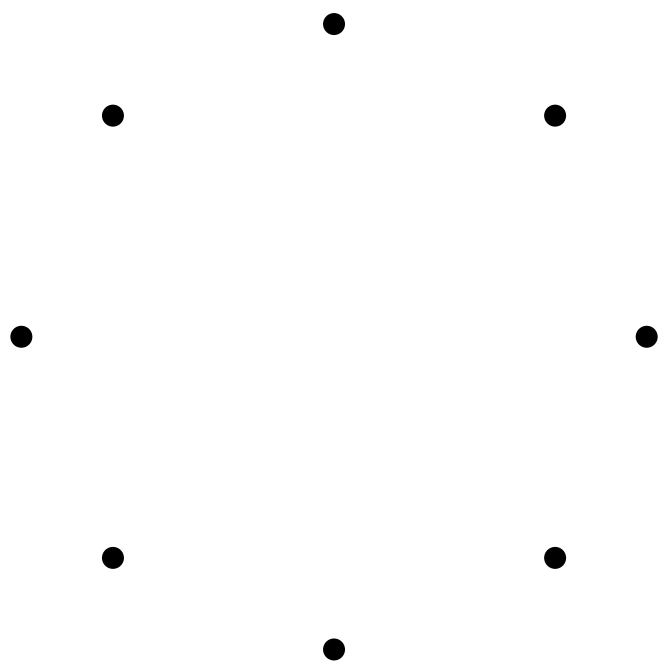
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$



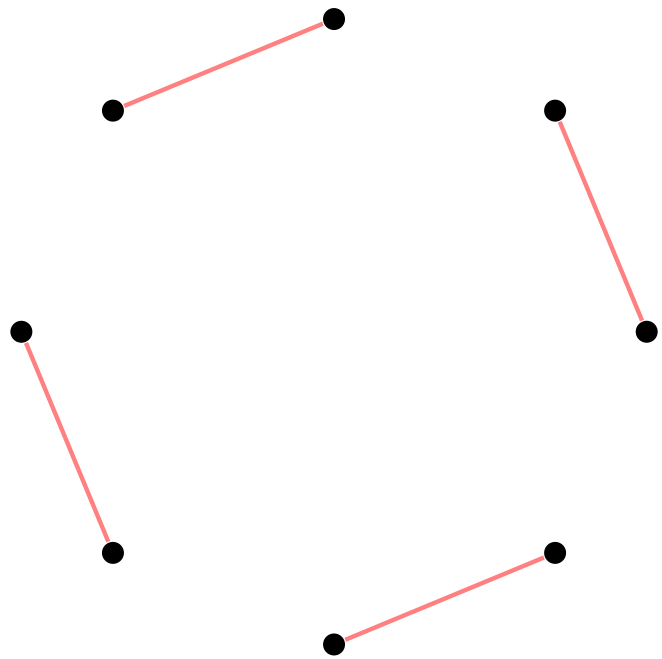
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 2$



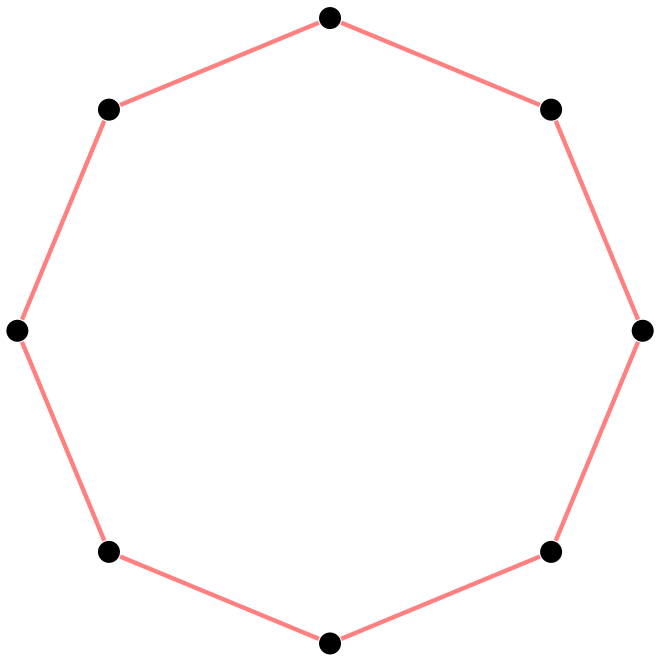
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 2$



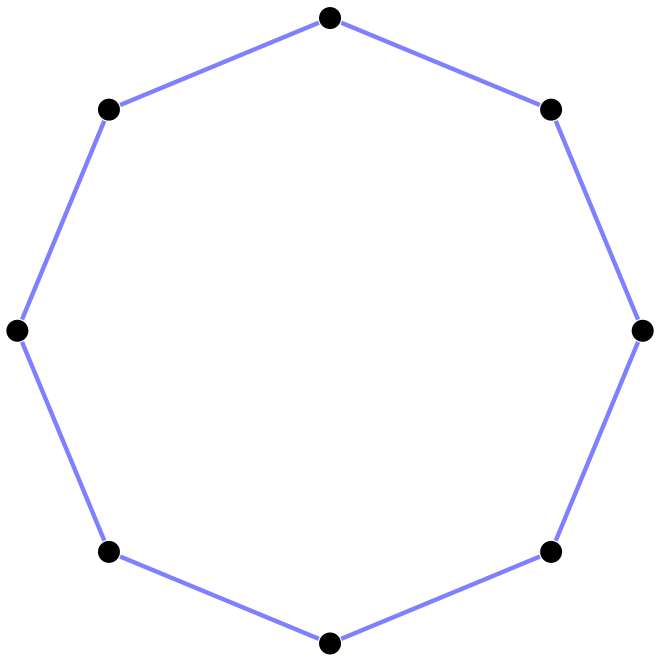
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 2$



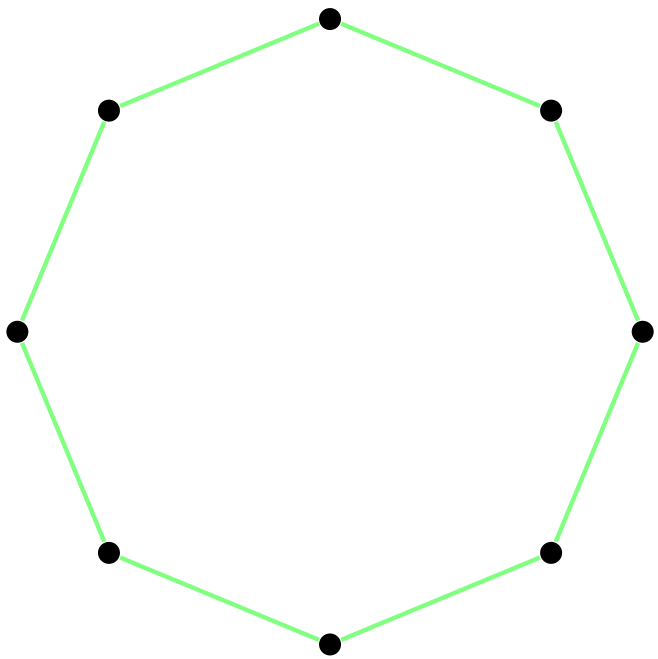
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 3$



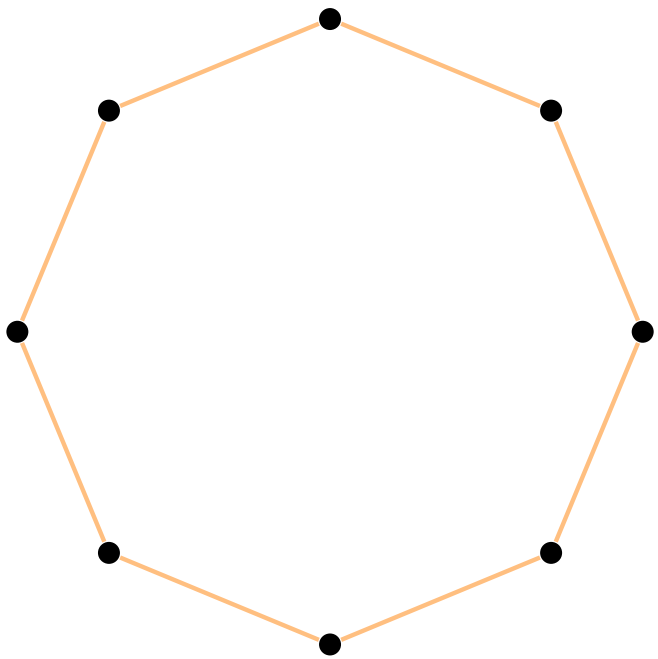
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 5$



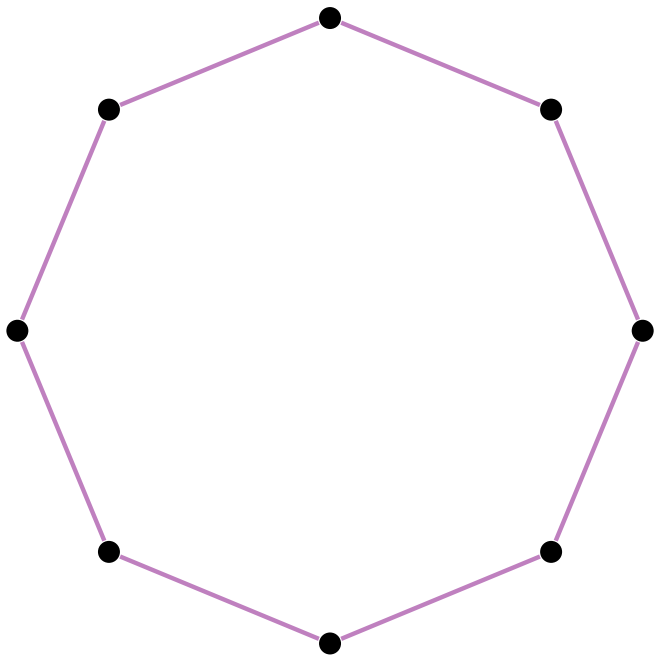
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 7$



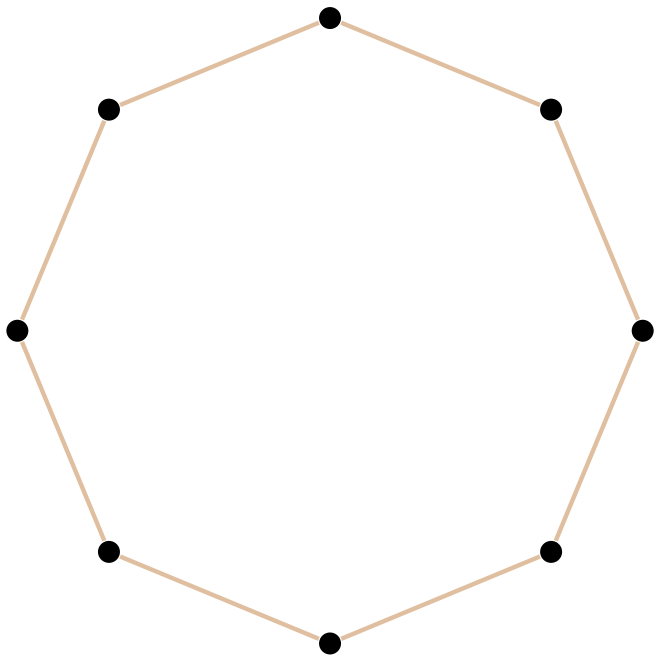
Elliptic curves & isogenies (1)

Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 11$

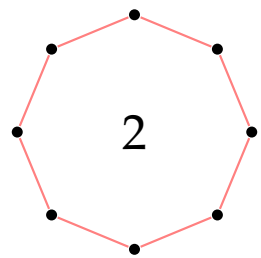


Elliptic curves & isogenies (1)

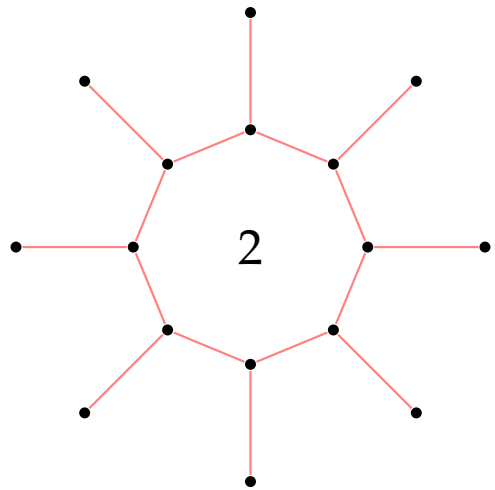
Fixed: prime p , $\mathrm{End}_{\mathbb{F}_p}(E_{a,b}) = \mathcal{O}_{\mathbb{Q}(\pi)}$, $\ell = 13$



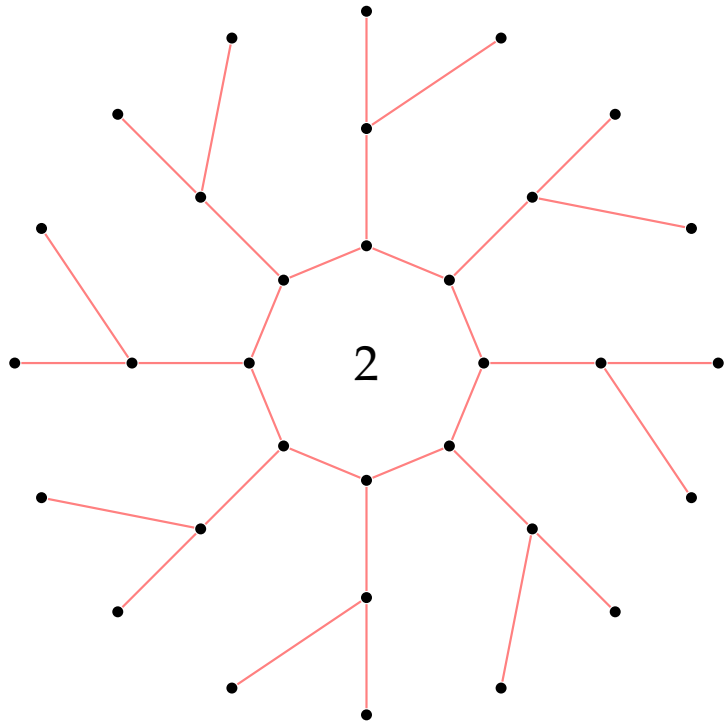
Elliptic curves & isogenies (2)



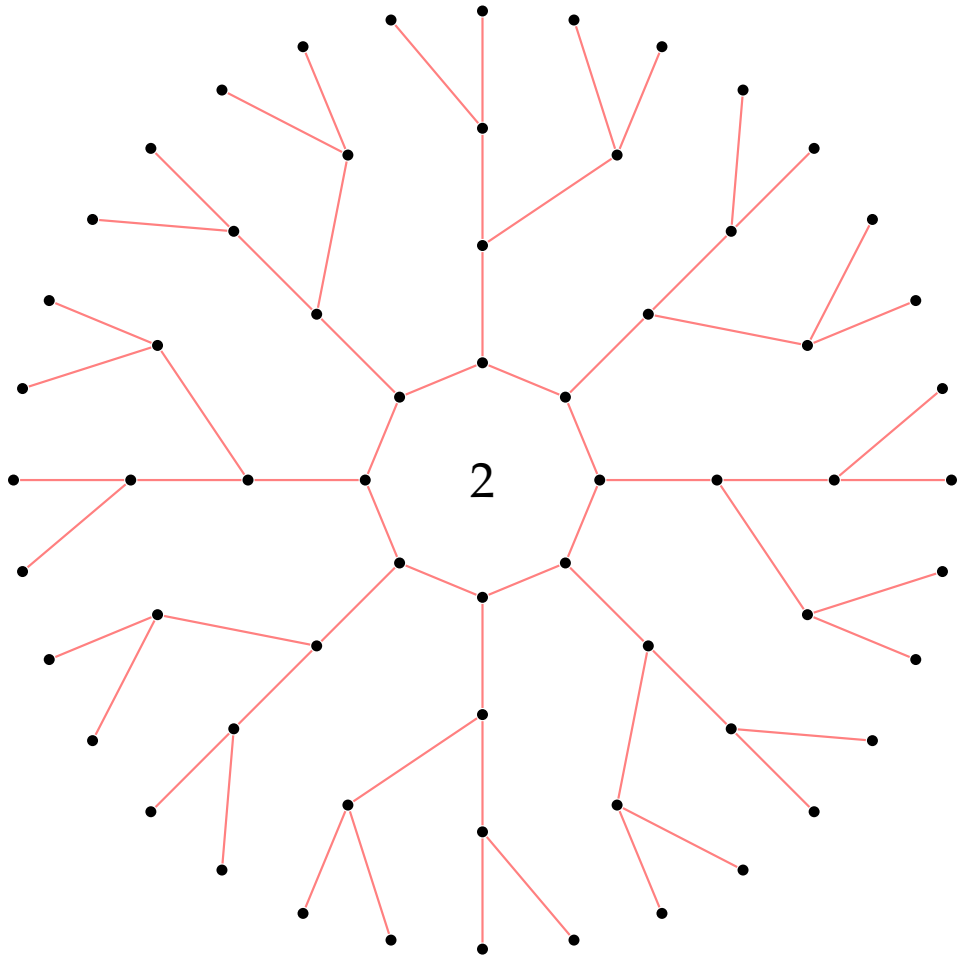
Elliptic curves & isogenies (2)



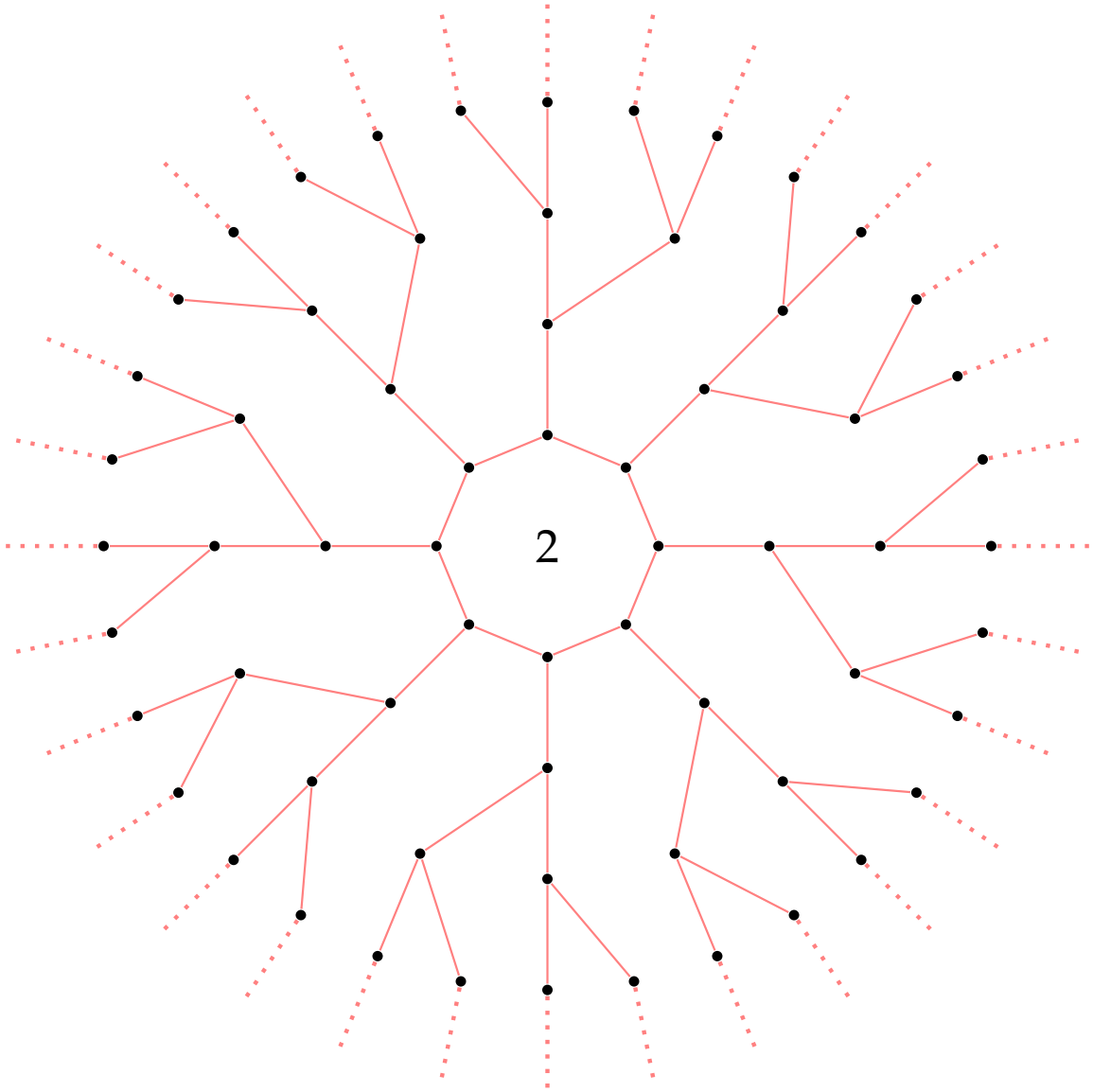
Elliptic curves & isogenies (2)



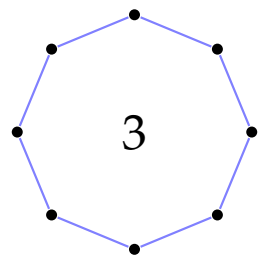
Elliptic curves & isogenies (2)



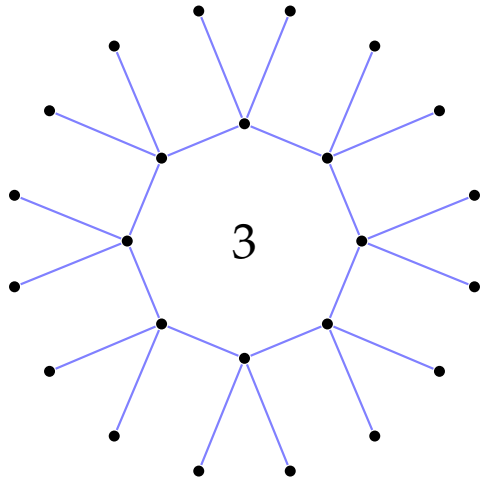
Elliptic curves & isogenies (2)



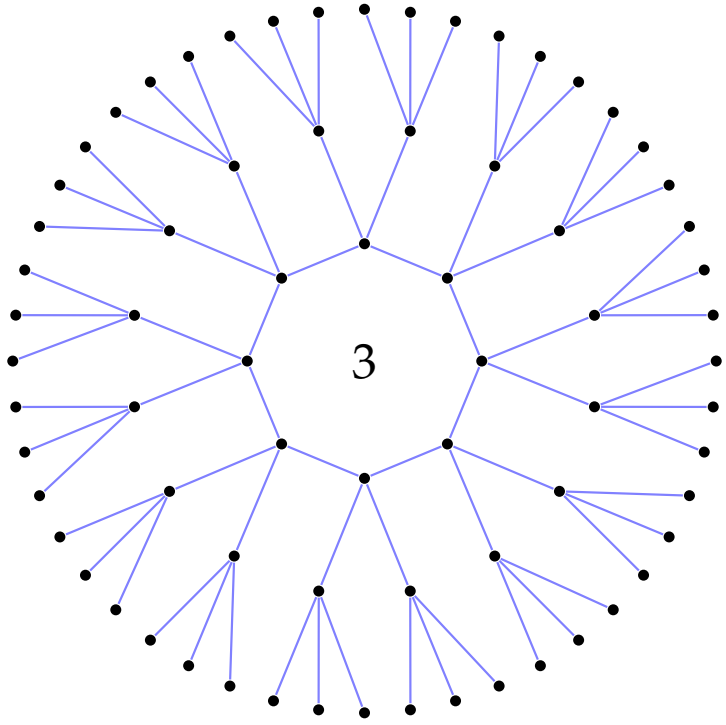
Elliptic curves & isogenies (2)



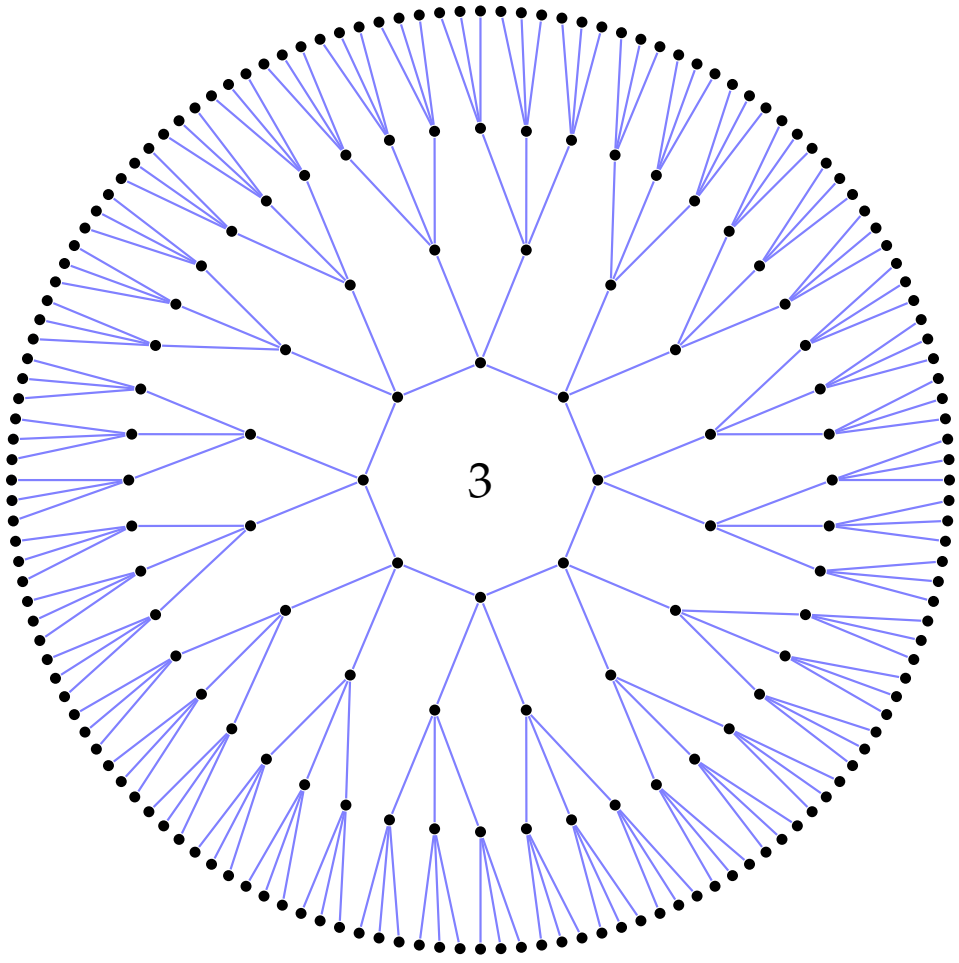
Elliptic curves & isogenies (2)



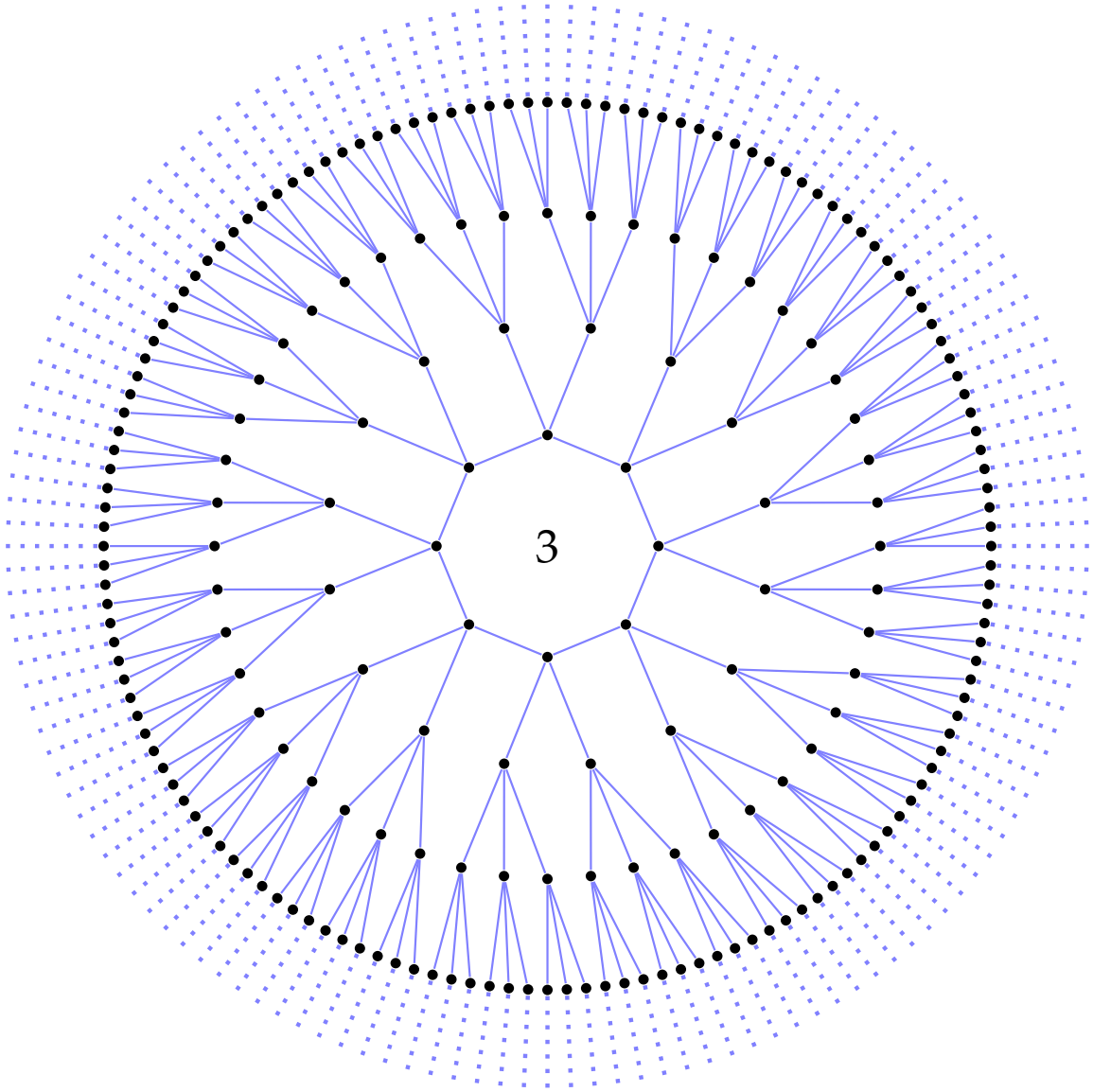
Elliptic curves & isogenies (2)



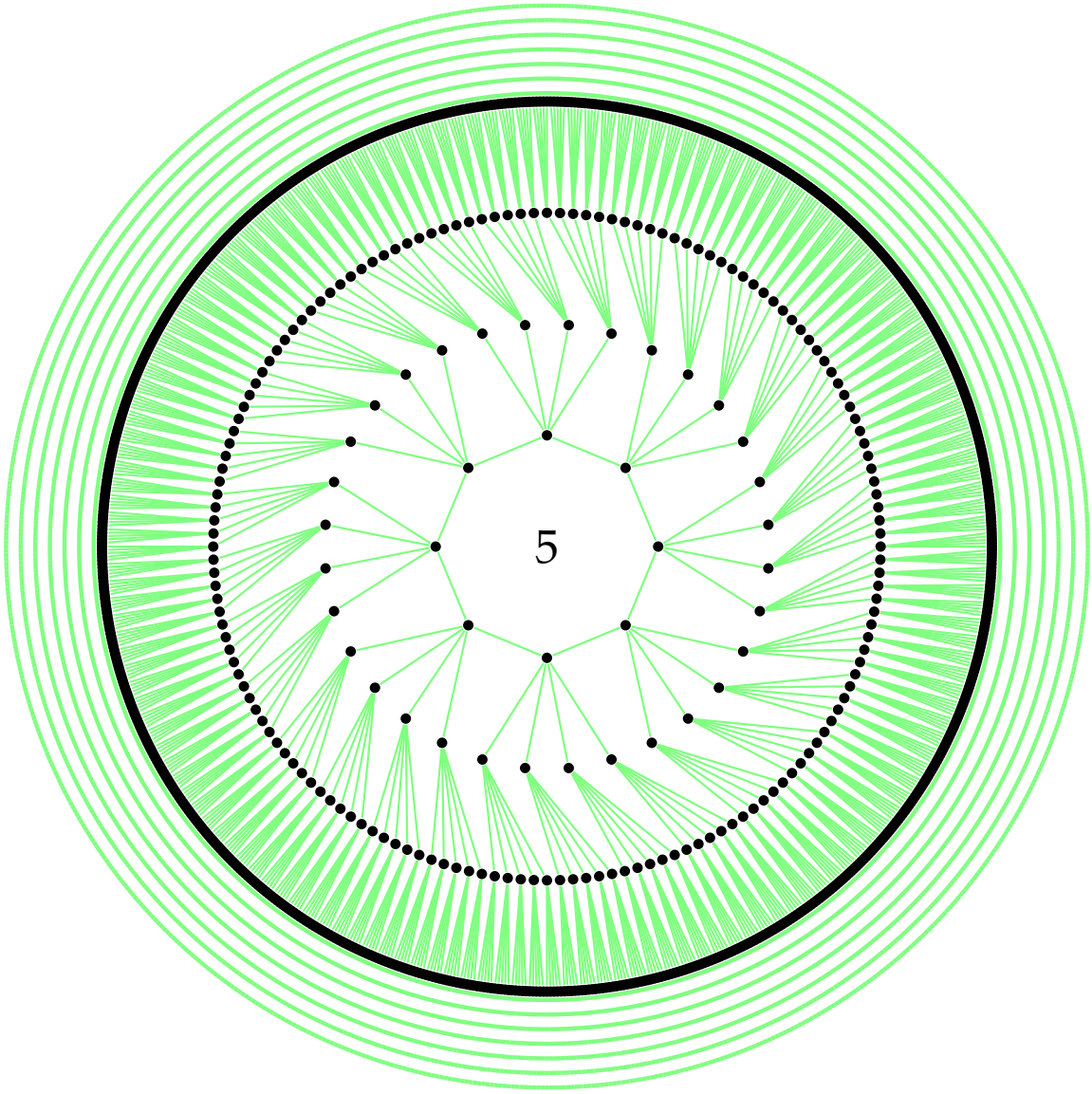
Elliptic curves & isogenies (2)



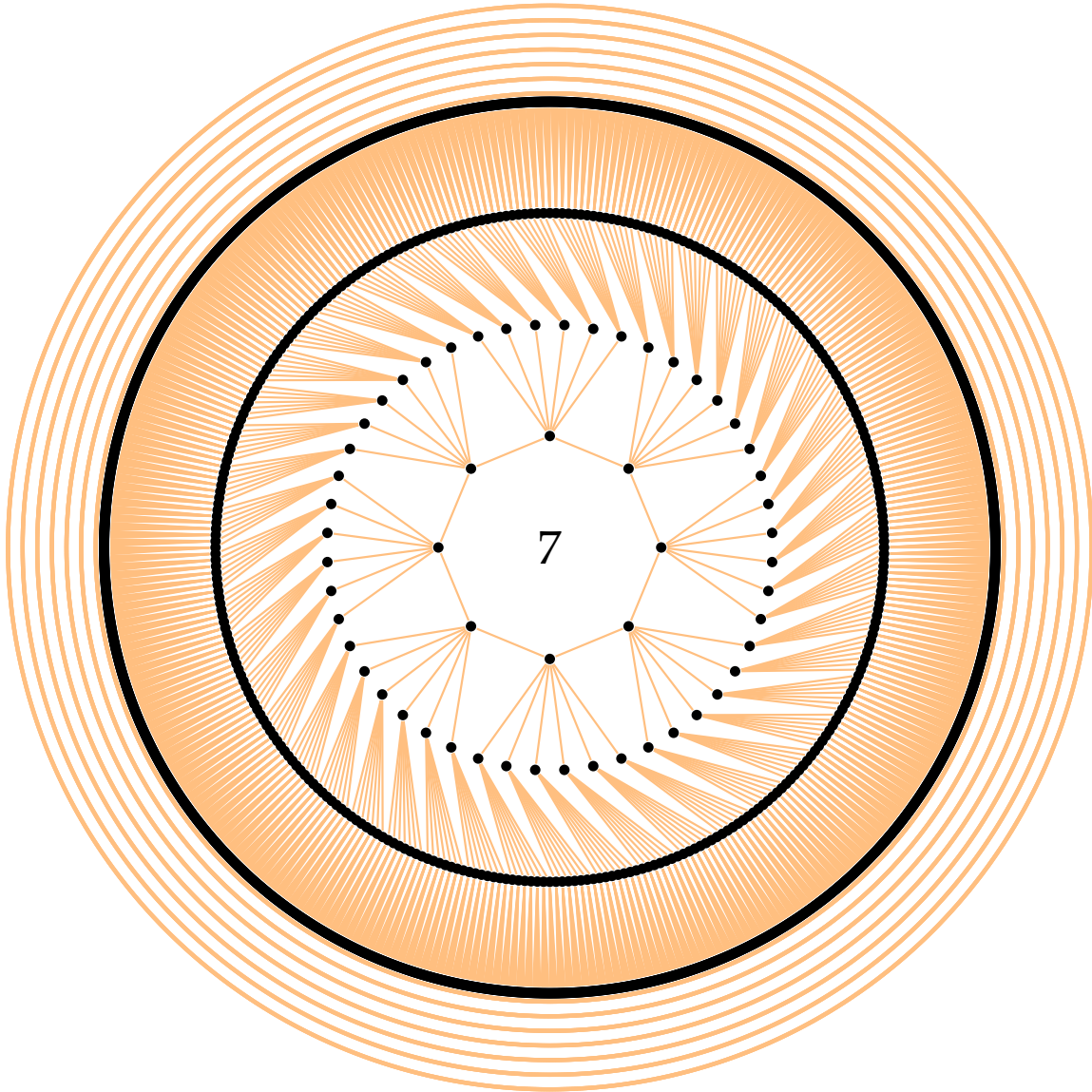
Elliptic curves & isogenies (2)



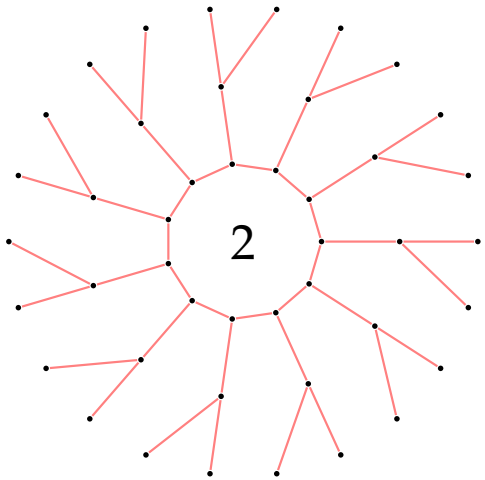
Elliptic curves & isogenies (2)

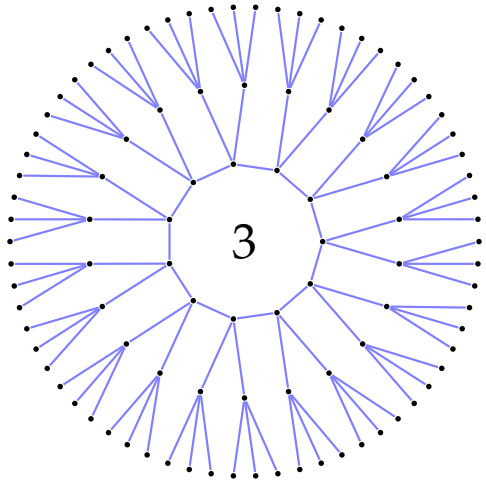


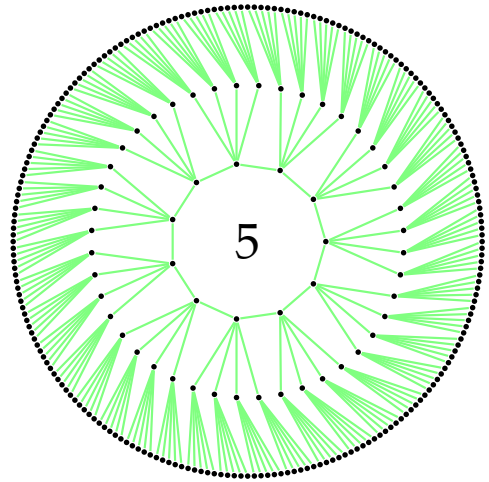
Elliptic curves & isogenies (2)

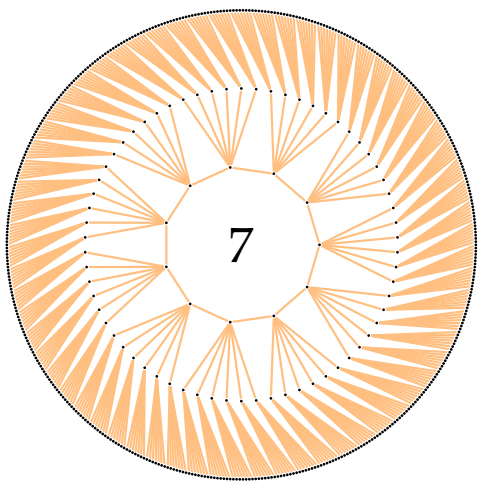


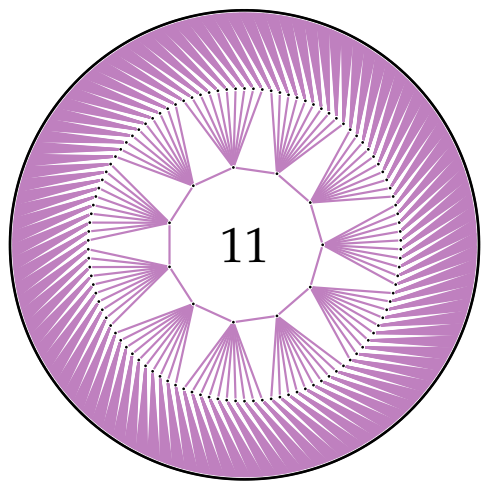
Isogeny volcanoes

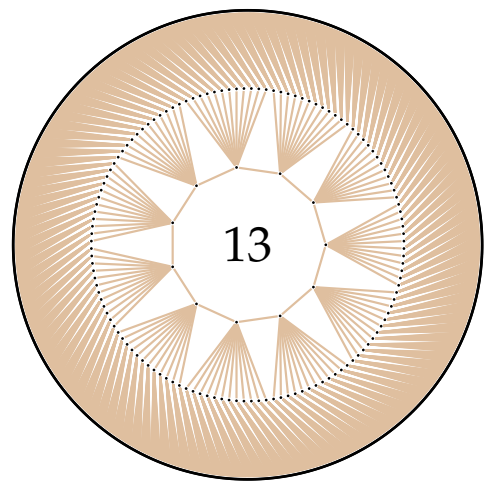




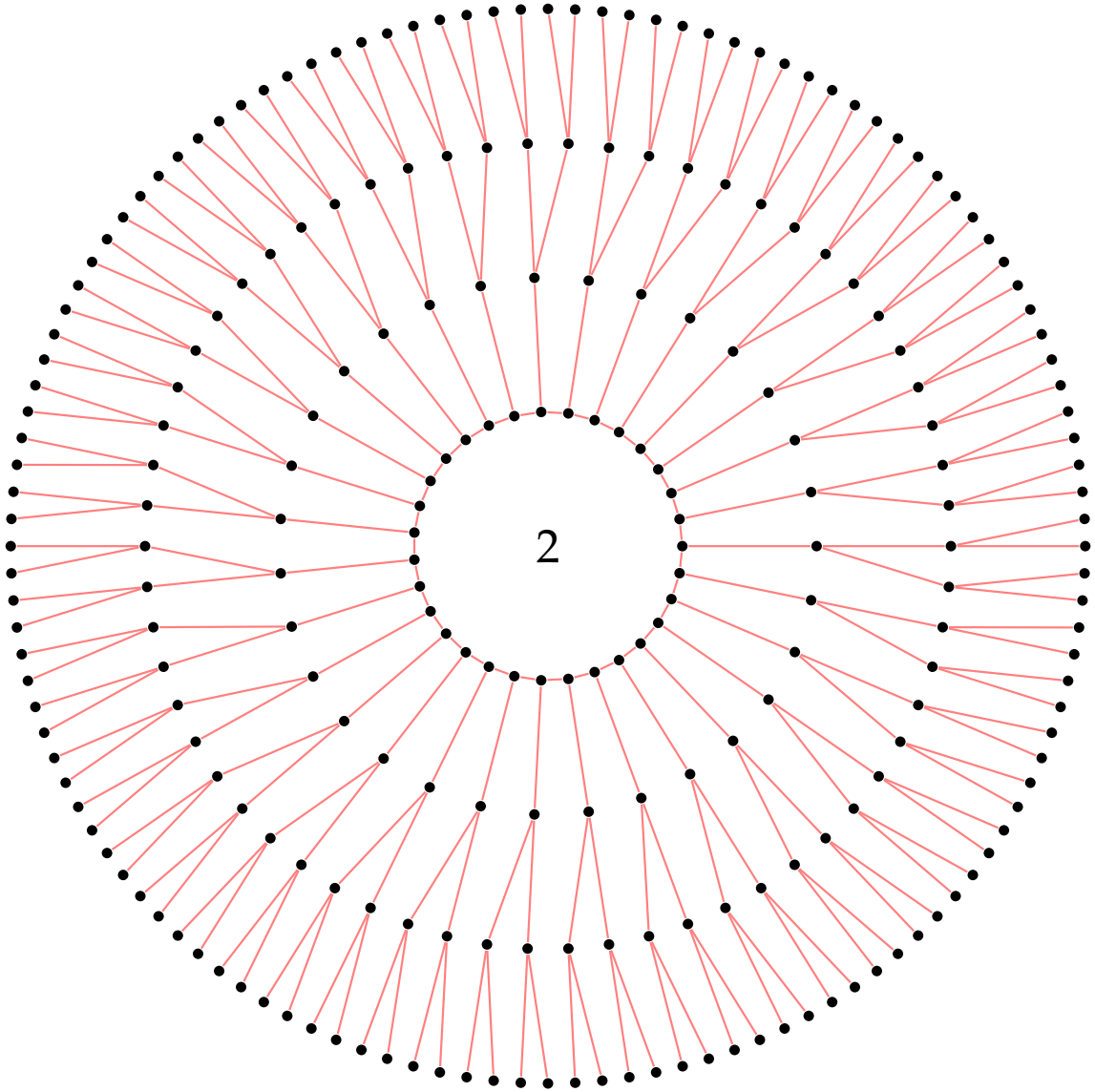




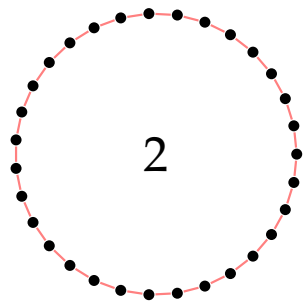




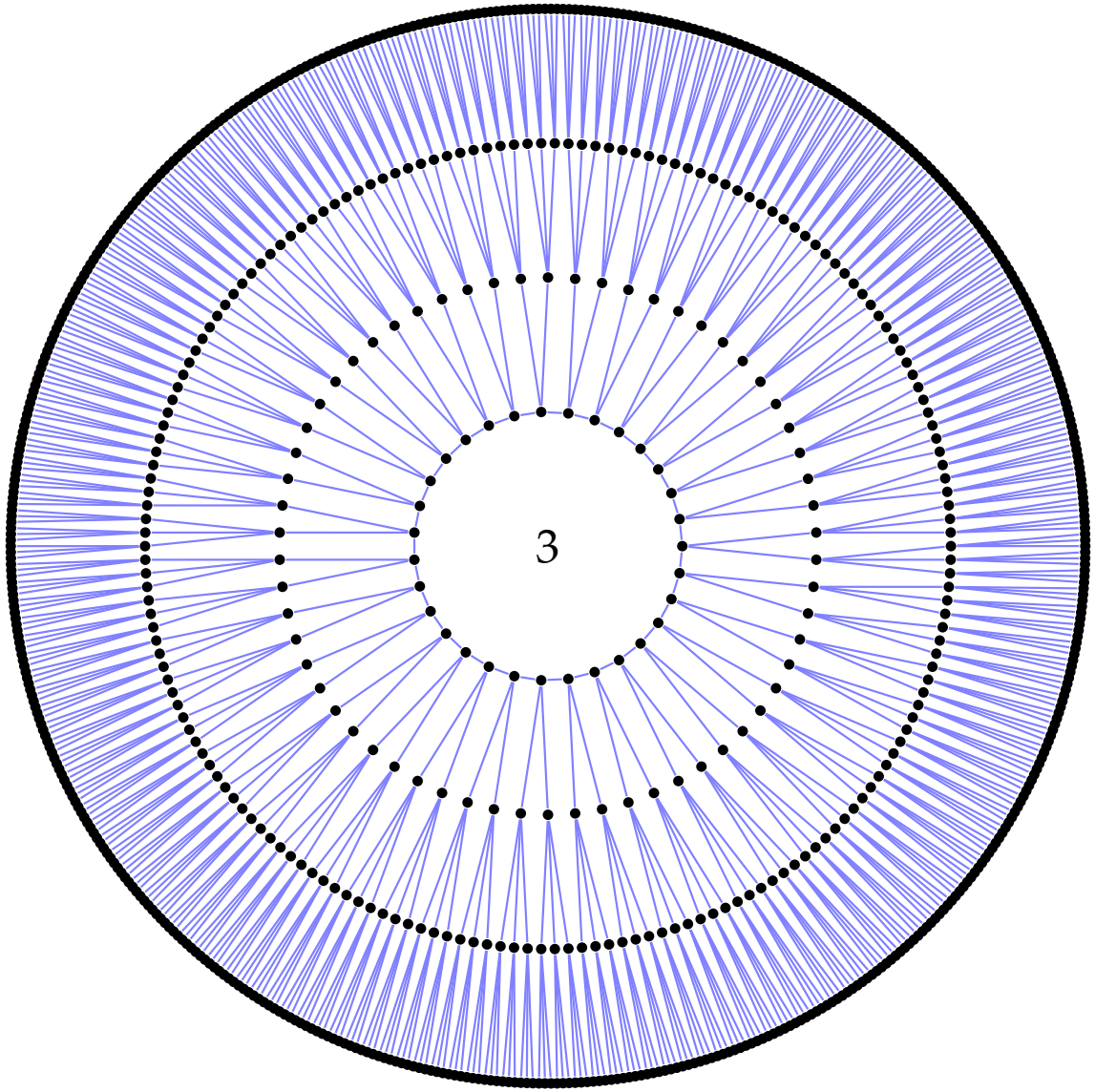
Isogeny-based cryptography (1)



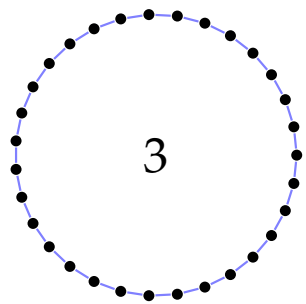
Isogeny-based cryptography (1)



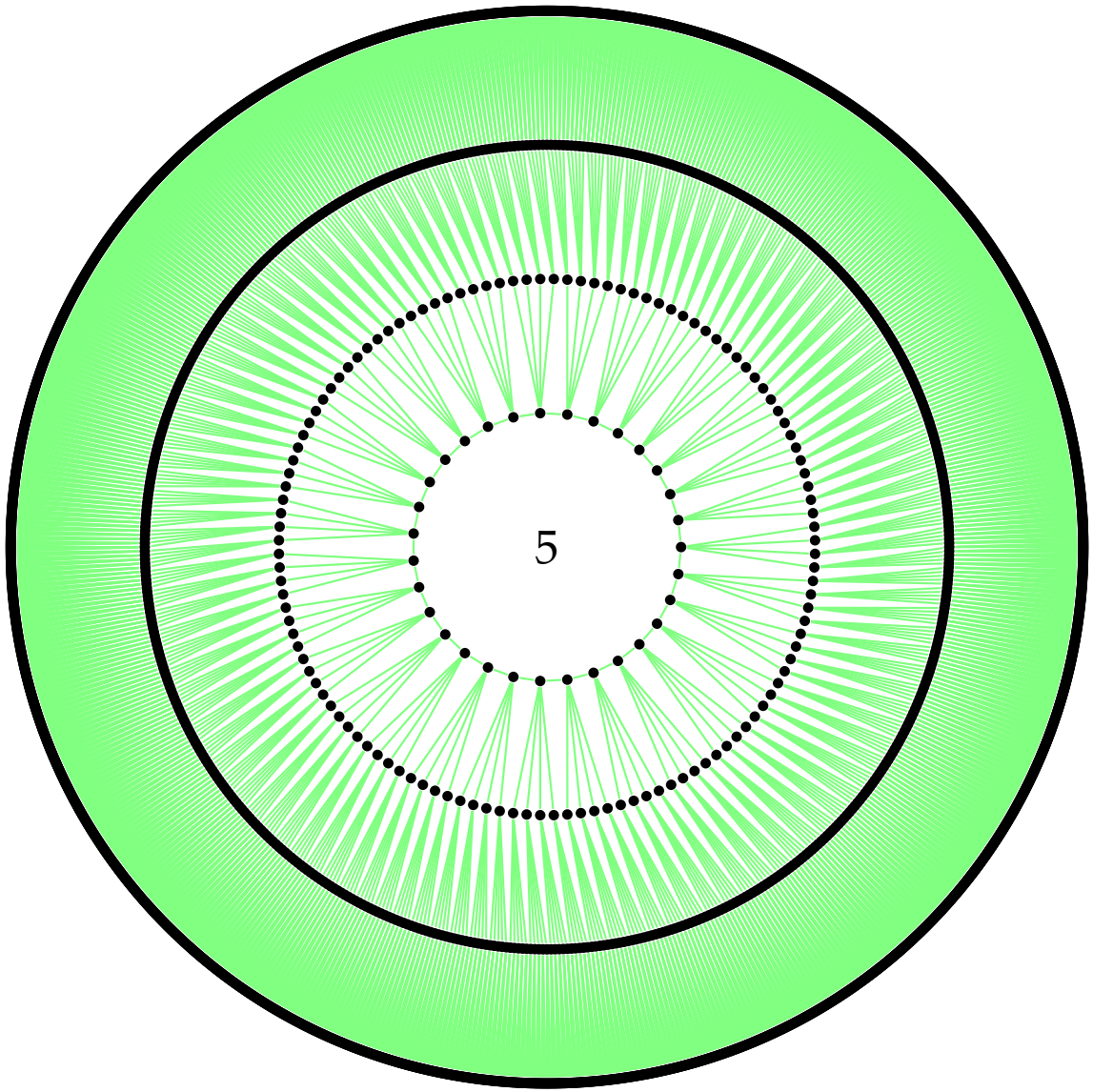
Isogeny-based cryptography (1)



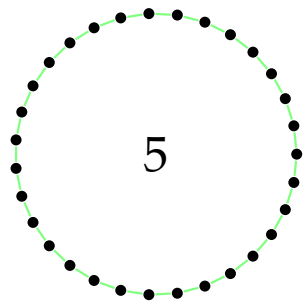
Isogeny-based cryptography (1)



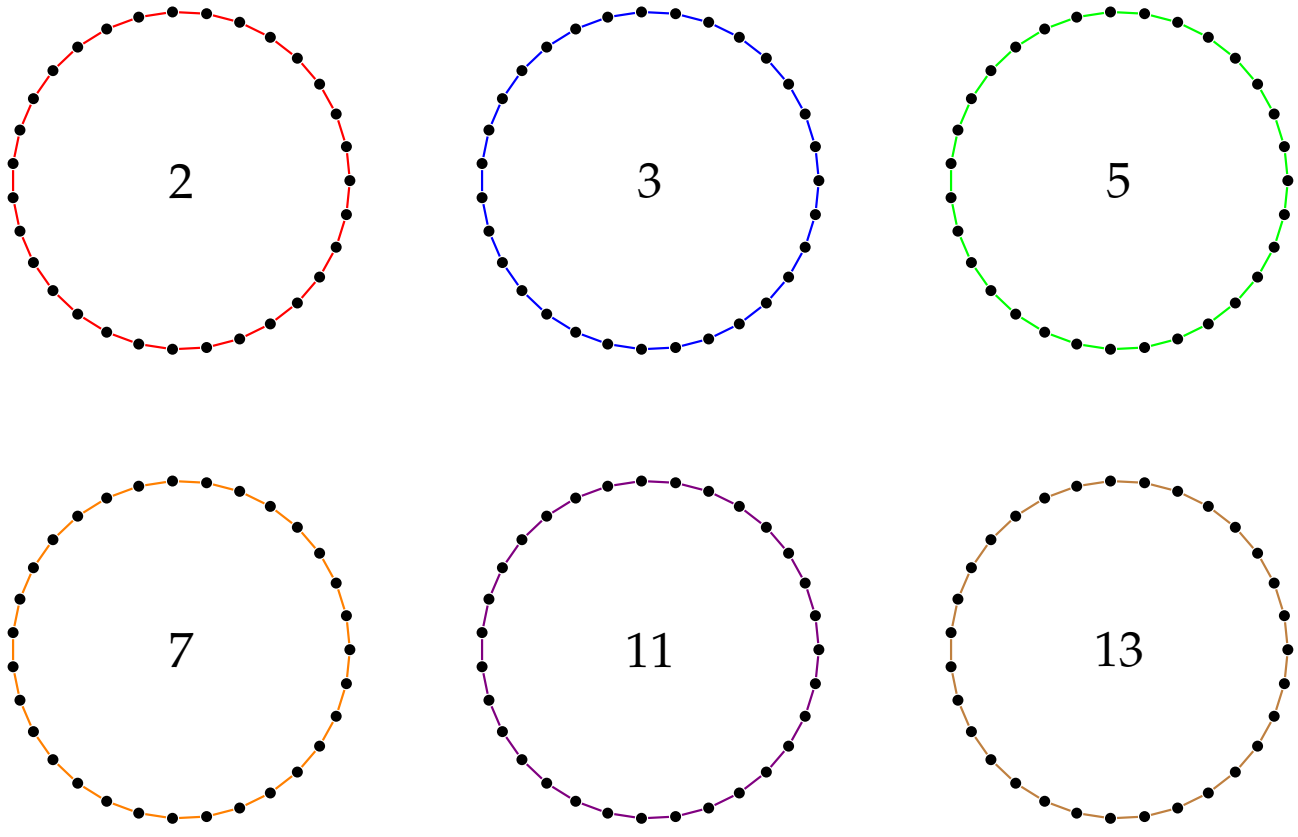
Isogeny-based cryptography (1)



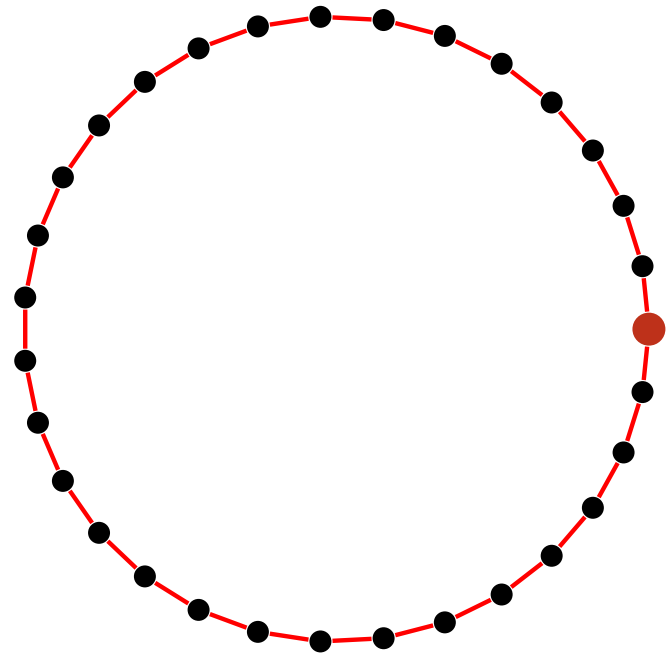
Isogeny-based cryptography (1)



Isogeny-based cryptography (1)

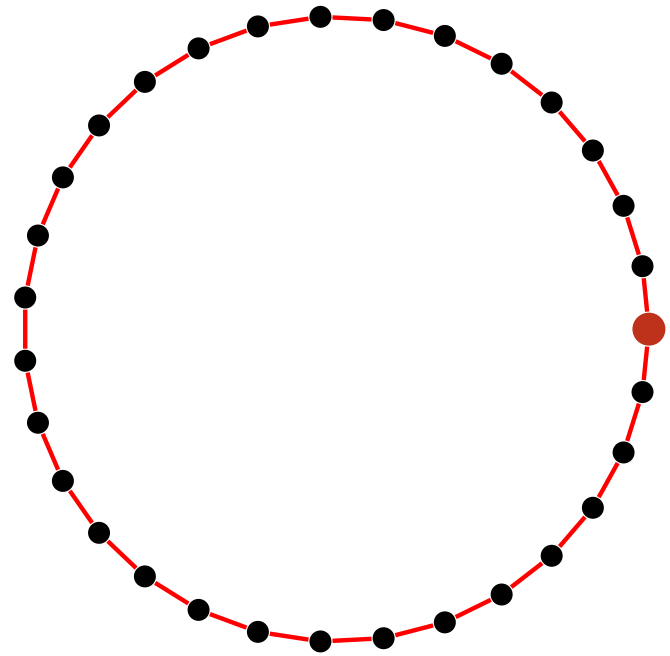


Isogeny-based cryptography (1)



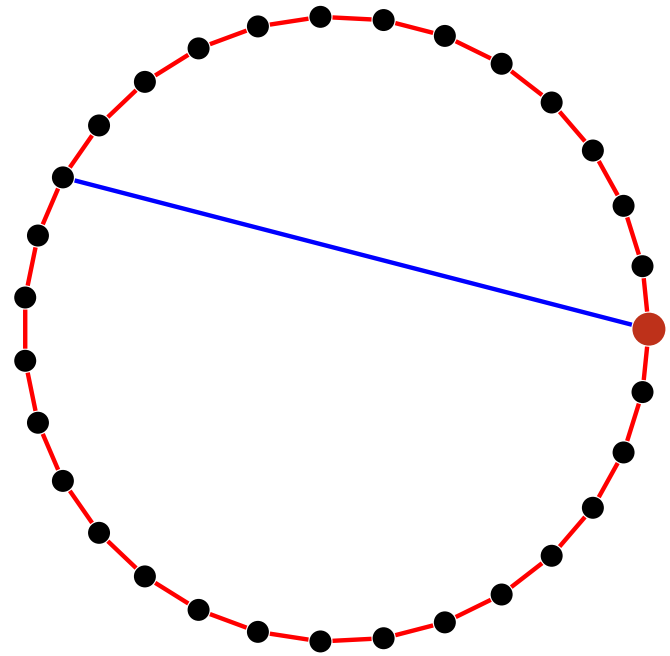
Isogeny-based cryptography (1)

# primes:	1
Work (per prime):	$\leq t$
Work (total):	$\leq t$
Entropy:	t



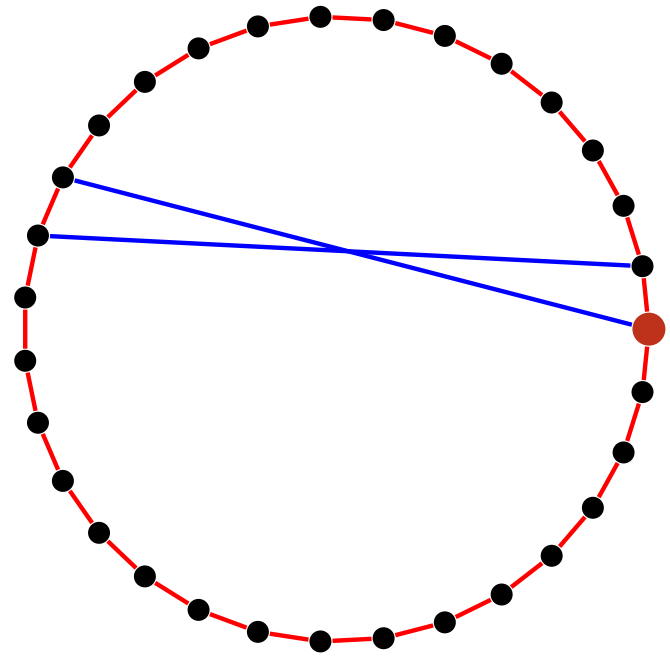
Isogeny-based cryptography (1)

# primes:	1
Work (per prime):	$\leq t$
Work (total):	$\leq t$
Entropy:	t



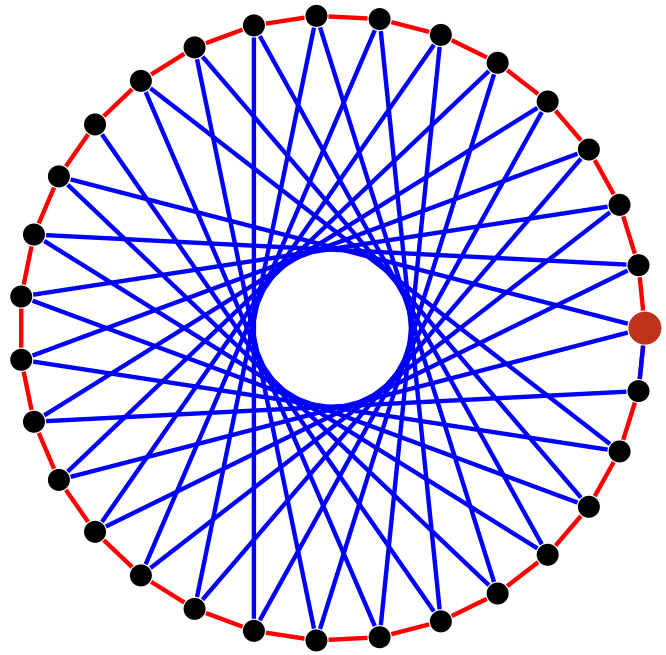
Isogeny-based cryptography (1)

# primes:	1
Work (per prime):	$\leq t$
Work (total):	$\leq t$
Entropy:	t



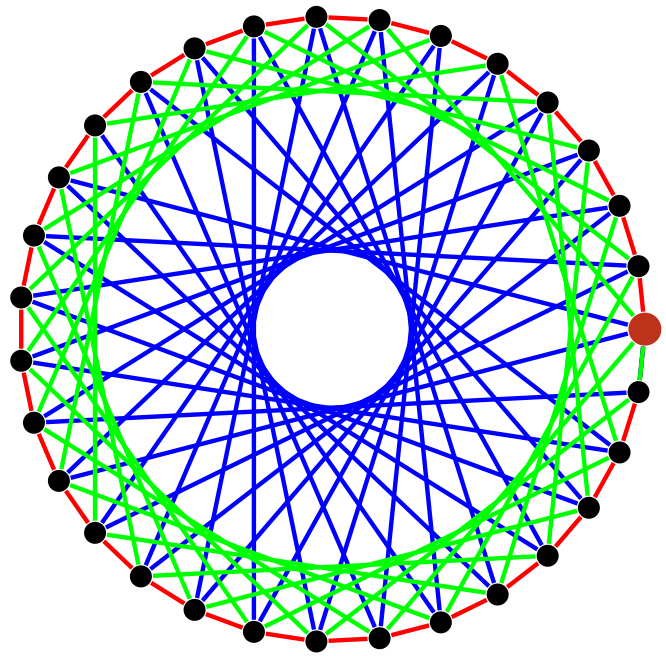
Isogeny-based cryptography (1)

# primes:	2
Work (per prime):	$\leq t$
Work (total):	$\leq 2 \cdot t$
Entropy:	t^2



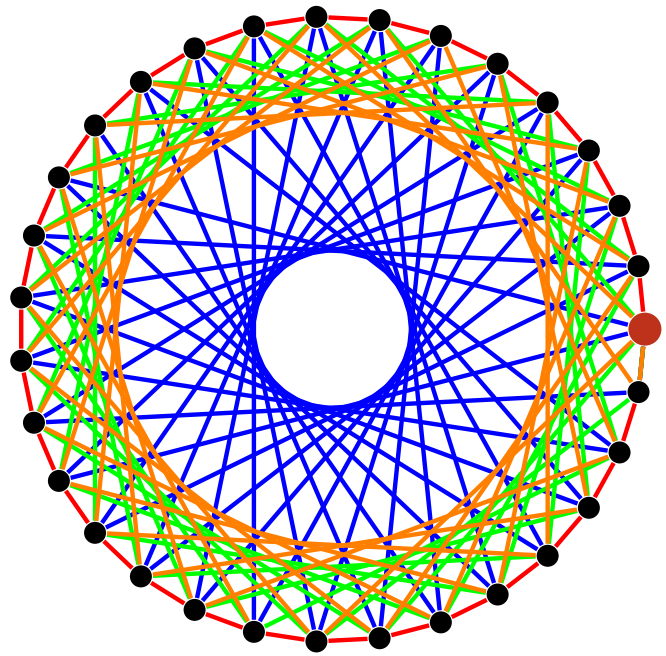
Isogeny-based cryptography (1)

# primes:	3
Work (per prime):	$\leq t$
Work (total):	$\leq 3 \cdot t$
Entropy:	t^3



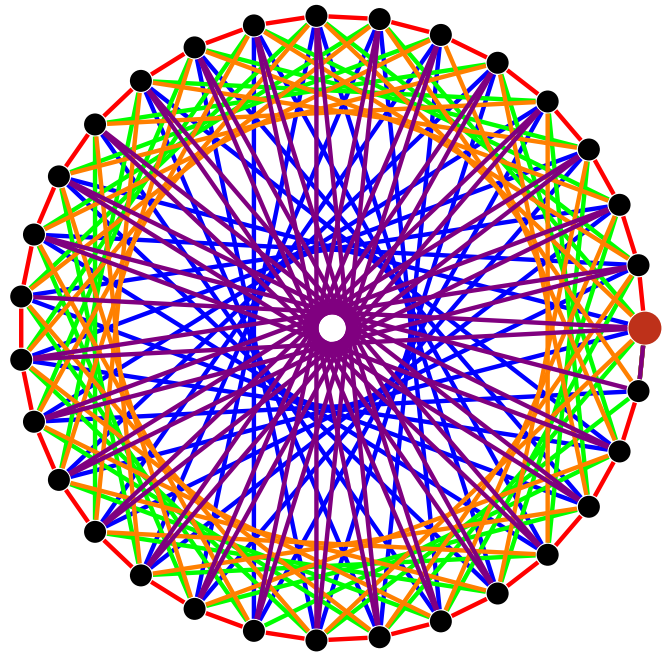
Isogeny-based cryptography (1)

# primes:	4
Work (per prime):	$\leq t$
Work (total):	$\leq 4 \cdot t$
Entropy:	t^4



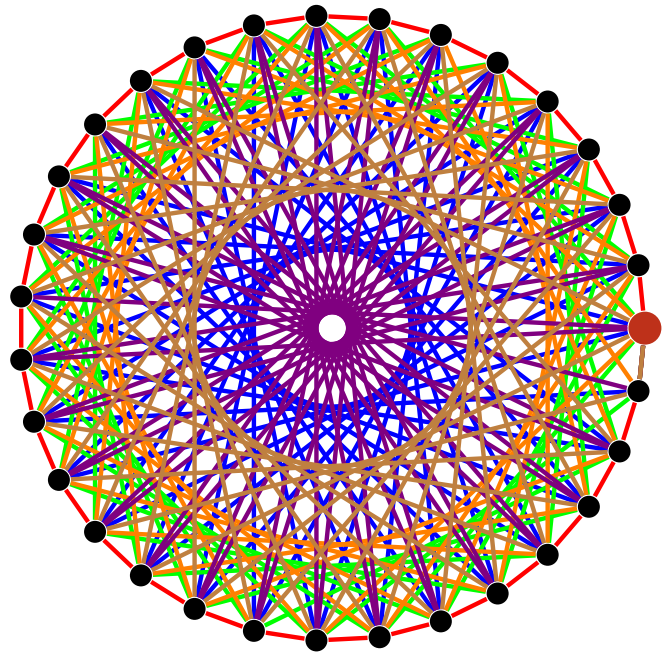
Isogeny-based cryptography (1)

# primes:	5
Work (per prime):	$\leq t$
Work (total):	$\leq 5 \cdot t$
Entropy:	t^5



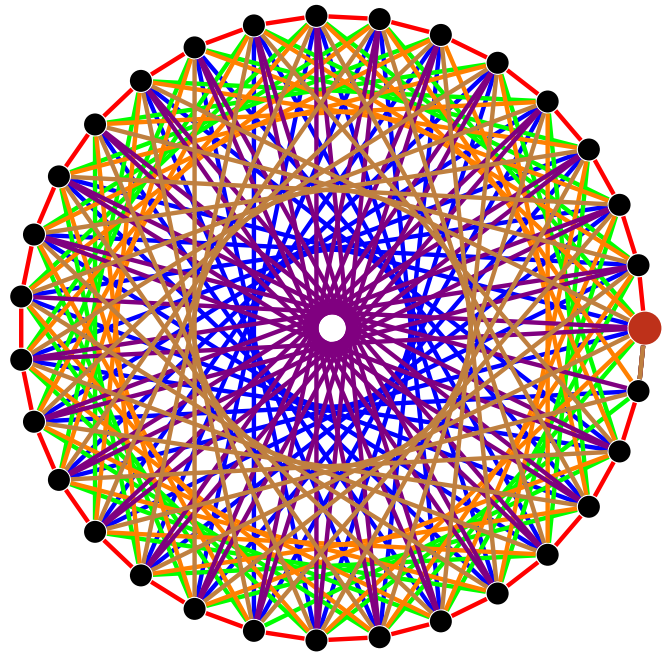
Isogeny-based cryptography (1)

# primes:	6
Work (per prime):	$\leq t$
Work (total):	$\leq 6 \cdot t$
Entropy:	t^6



Isogeny-based cryptography (1)

# primes:	L
Work (per prime):	$\leq t$
Work (total):	$\leq L \cdot t$
Entropy:	t^L



OIDH & CSIDH

Two different ways to instantiate;

1. *Ordinary* isogeny Diffie–Hellman (OIDH)
2. *Supersingular* isogeny Diffie–Hellman (CSIDH)

The idea for OIDH first by Couveignes in ’96 [Cou06]

$\Longrightarrow$ Post-quantum security with very small keys [DKS18]

$\Longrightarrow$ CSIDH almost identical but easier to instantiate [Cas+18]

State of CSIDH

($\sim$ NIST level I security)

1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)

State of CSIDH

($\sim$ NIST level I security)

1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)
2. Constant-time implementations [MCR18] (at $\sim$ 246 ms)

State of CSIDH

($\sim$ NIST level I security)

1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)
2. Constant-time implementations [MCR18] (at $\sim$ 246 ms)
3. **SeaSign** signatures [DG19] *large* and/or *slow*

State of CSIDH

($\sim$ NIST level I security)

1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)
2. Constant-time implementations [MCR18] (at $\sim$ 246 ms)
3. **SeaSign** signatures [DG19] *large* and/or *slow*
4. **CSI-FiSh** signatures [BKV19] *smaller* and *faster* (small p)

State of CSIDH

($\sim$ NIST level I security)

1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)
2. Constant-time implementations [MCR18] (at $\sim$ 246 ms)
3. **SeaSign** signatures [DG19] *large* and/or *slow*
4. **CSI-FiSh** signatures [BKV19] *smaller* and *faster* (small p)
5. Bunch of cryptanalysis [BS18; Ber+19]
   - Quantum subexponential attacks!

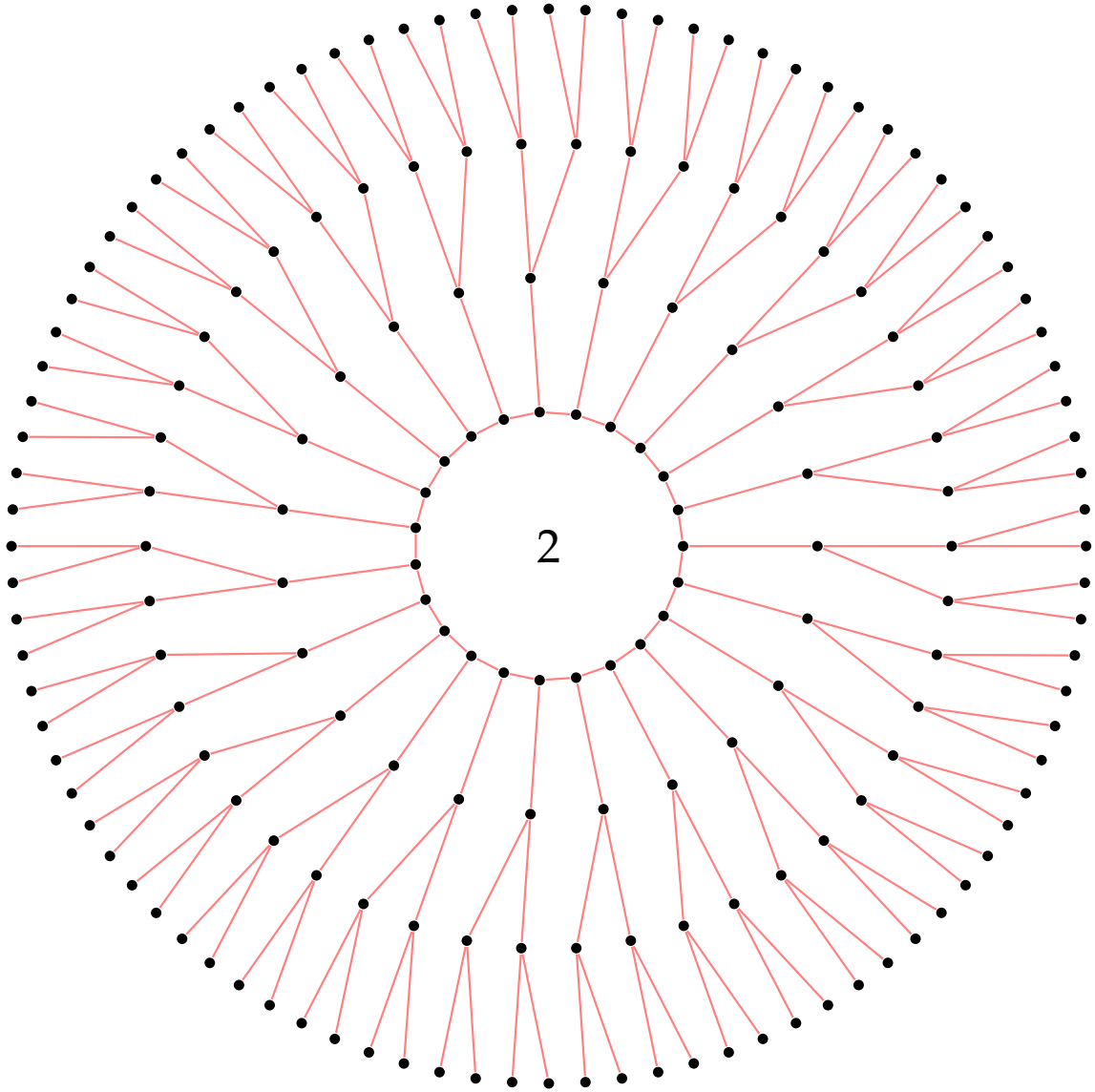
State of CSIDH

($\sim$ NIST level I security)

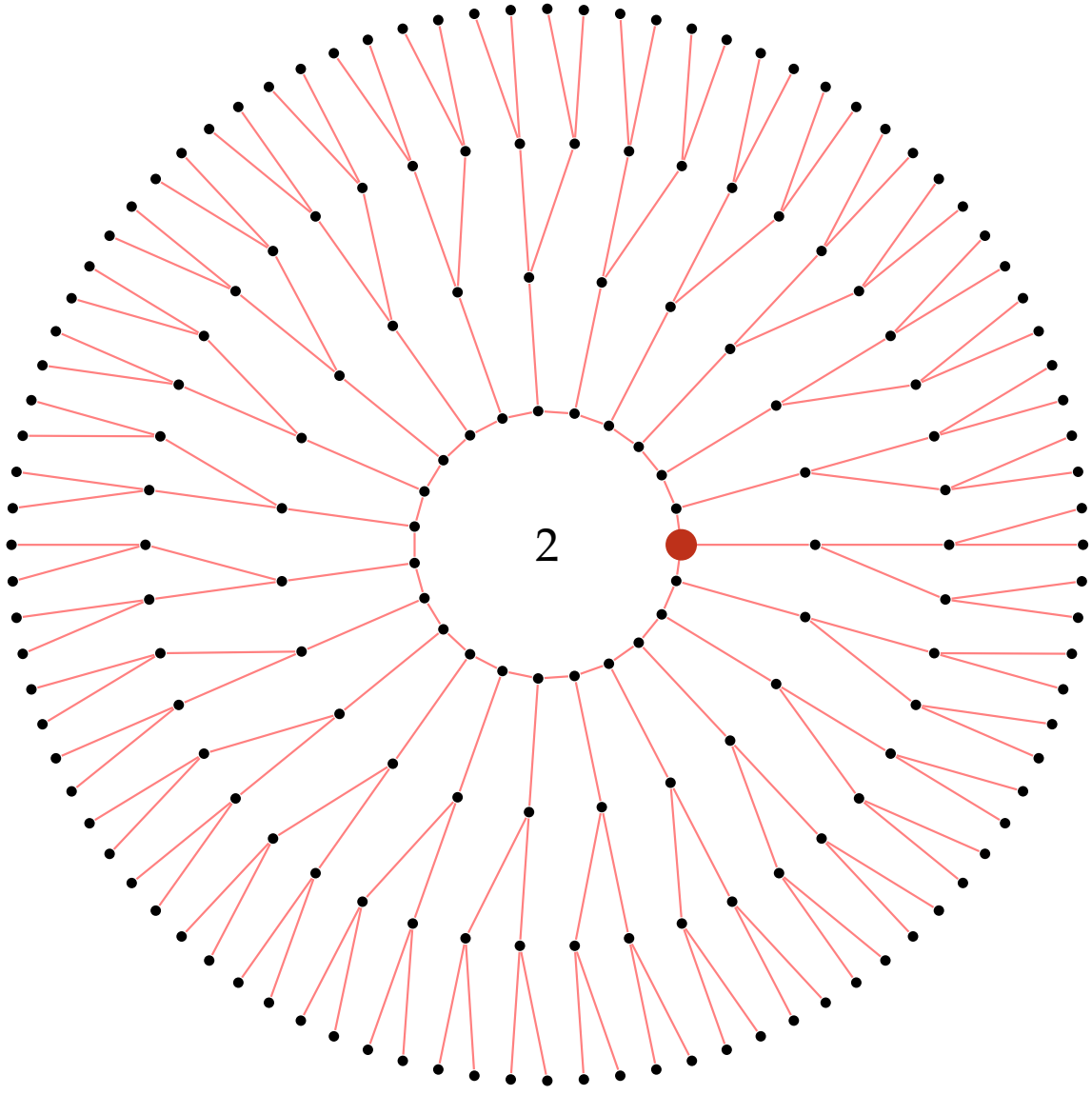
1. **CSIDH** key exchange
   - *Non-interactive* with 64-byte public keys
   - $\sim$ 80 ms for full exchange (not constant-time)
2. Constant-time implementations [MCR18] (at $\sim$ 246 ms)
3. **SeaSign** signatures [DG19] *large* and/or *slow*
4. **CSI-FiSh** signatures [BKV19] *smaller* and *faster* (small p)
5. Bunch of cryptanalysis [BS18; Ber+19]
   - Quantum subexponential attacks!

Lots of stuff coming out!

Isogeny-based cryptography (2)



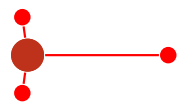
Isogeny-based cryptography (2)



Isogeny-based cryptography (2)

Isogeny-based cryptography (2)

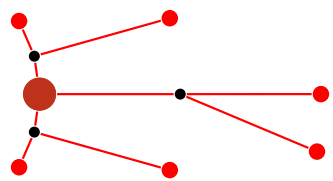
# primes:	1 ($\ell = 2$)
Work (per prime):	1
Work (total):	1
Entropy:	3

2 

Isogeny-based cryptography (2)

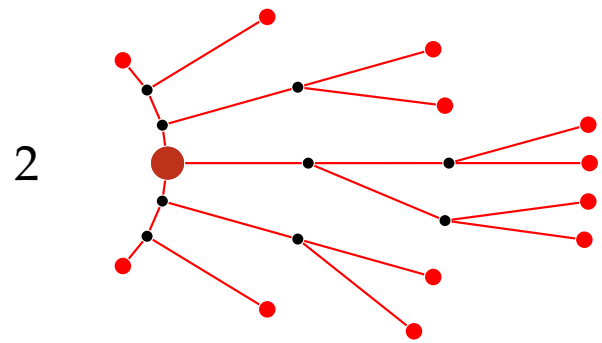
# primes:	1 $(\ell = 2)$
Work (per prime):	2
Work (total):	2
Entropy:	$3 \cdot 2$

2



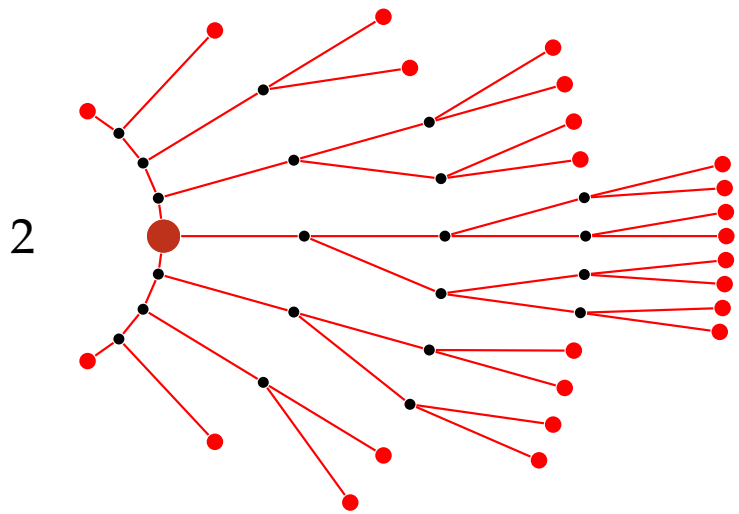
Isogeny-based cryptography (2)

# primes:	1 $(\ell = 2)$
Work (per prime):	3
Work (total):	3
Entropy:	$3 \cdot 2^2$



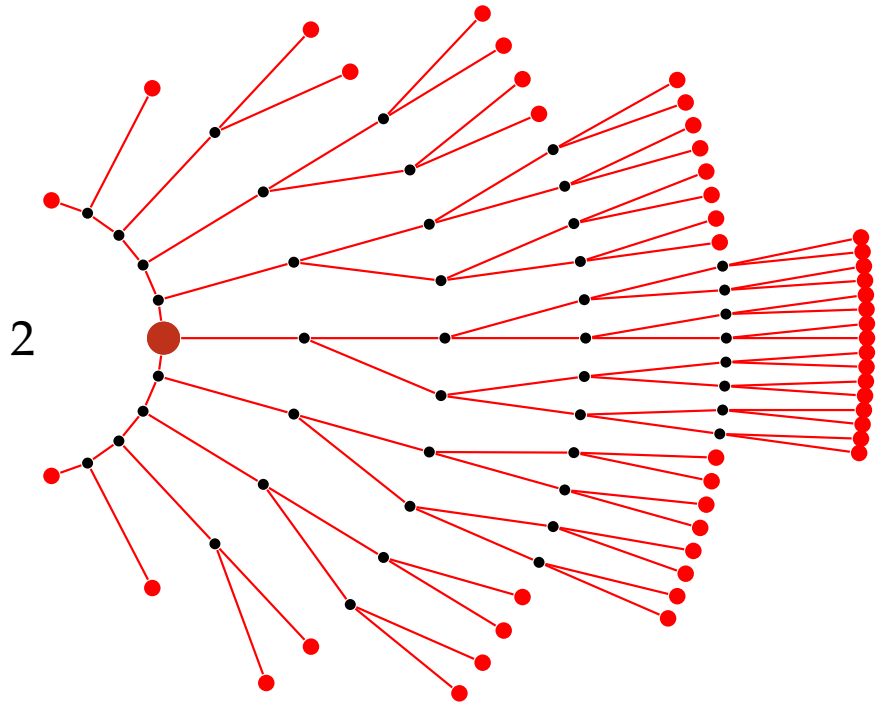
Isogeny-based cryptography (2)

# primes:	1 $(\ell = 2)$
Work (per prime):	4
Work (total):	4
Entropy:	$3 \cdot 2^3$



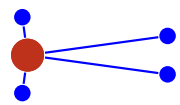
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 2$)
Work (per prime):	5
Work (total):	5
Entropy:	$3 \cdot 2^4$



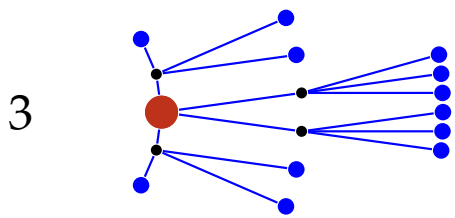
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 3$)
Work (per prime):	1
Work (total):	1
Entropy:	4

3 

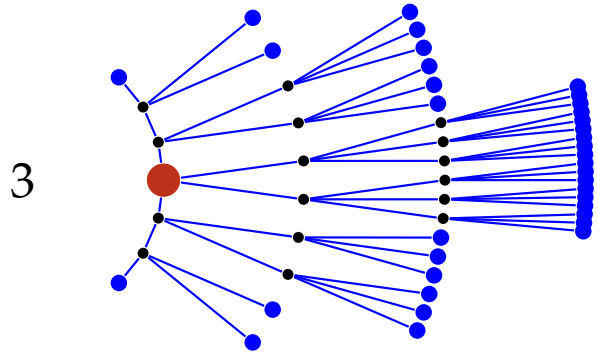
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 3$)
Work (per prime):	2
Work (total):	2
Entropy:	$4 \cdot 3$



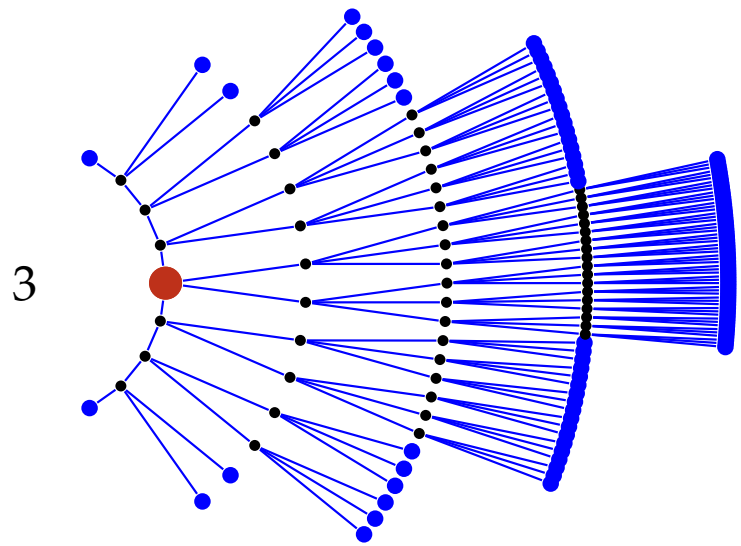
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 3$)
Work (per prime):	3
Work (total):	3
Entropy:	$4 \cdot 3^2$



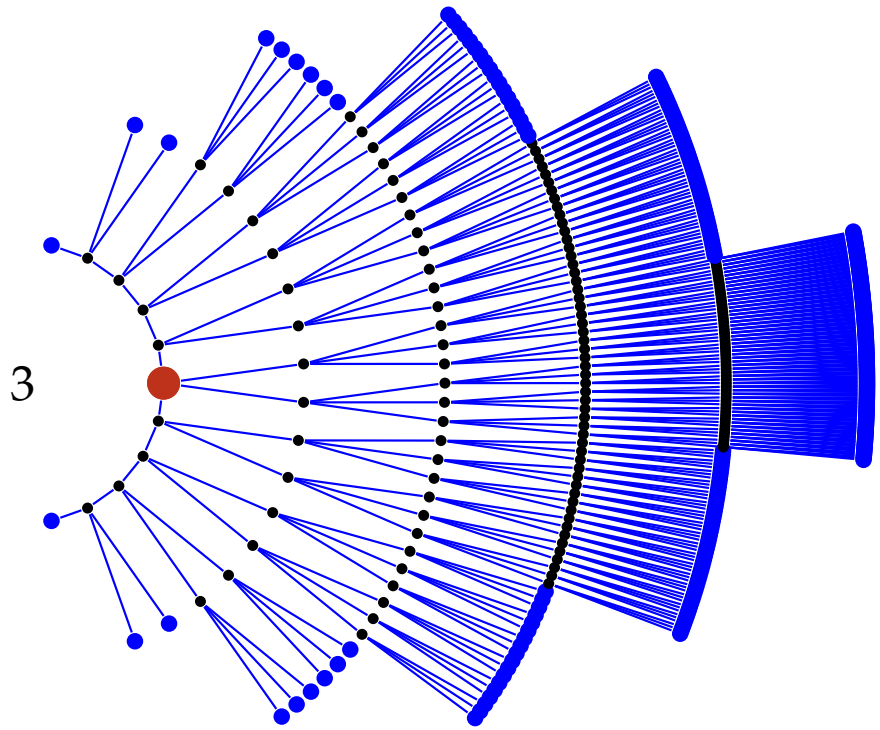
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 3$)
Work (per prime):	4
Work (total):	4
Entropy:	$4 \cdot 3^3$



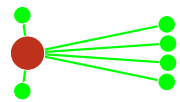
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 3$)
Work (per prime):	5
Work (total):	5
Entropy:	$4 \cdot 3^4$



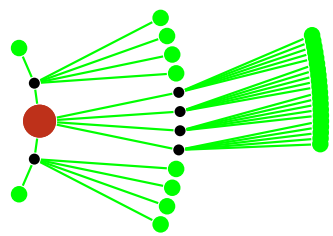
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 5$)
Work (per prime):	1
Work (total):	1
Entropy:	5

5 

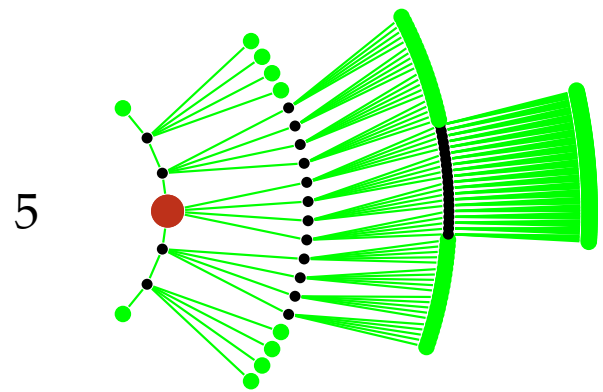
Isogeny-based cryptography (2)

# primes:	1 ($\ell = 5$)
Work (per prime):	2
Work (total):	2
Entropy:	$6 \cdot 5$



Isogeny-based cryptography (2)

# primes:	1 $(\ell = 5)$
Work (per prime):	3
Work (total):	3
Entropy:	$6 \cdot 5^2$

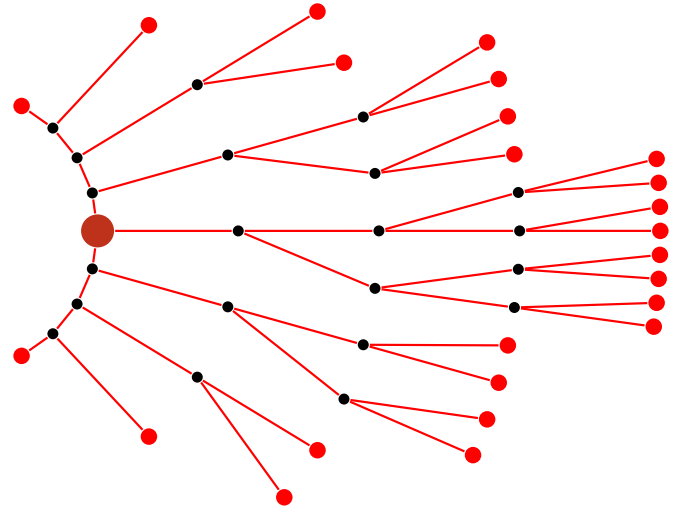


Isogeny-based cryptography (2)

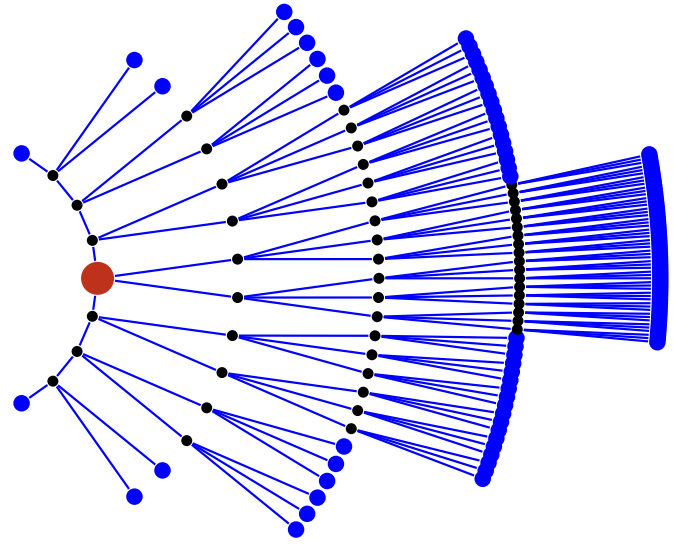
# primes:	1
Work (per prime):	t
Work (total):	t
Entropy:	$\sim \ell^t$

Isogeny-based cryptography (2)

Alice: 2

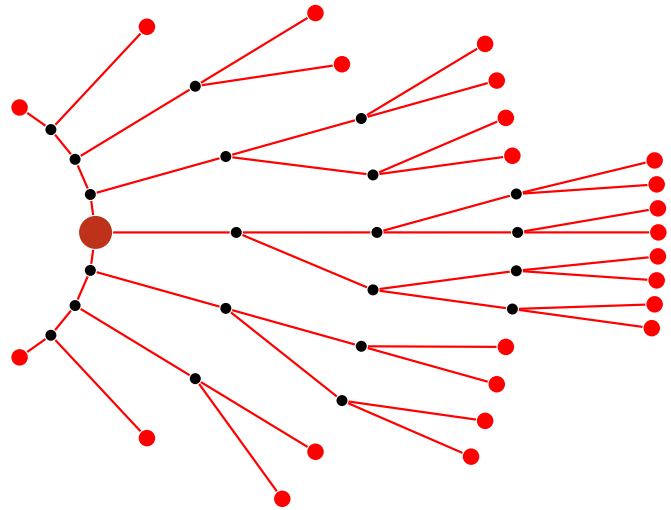


Bob: 3

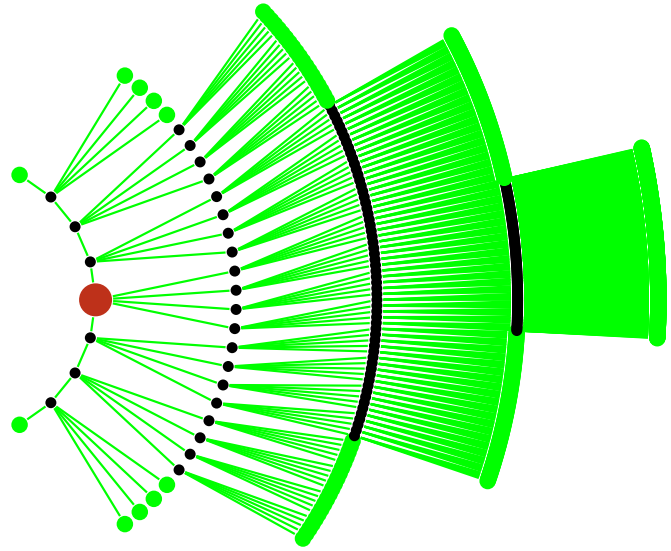


Isogeny-based cryptography (2)

Alice: 2

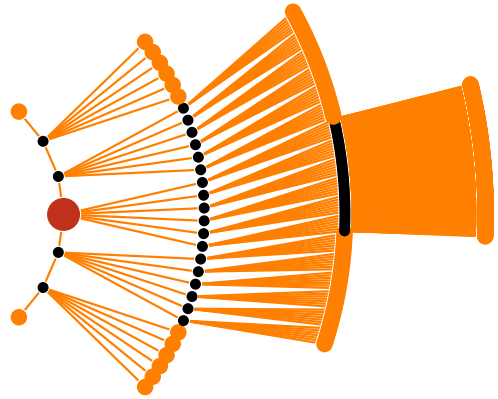


Bob: 5

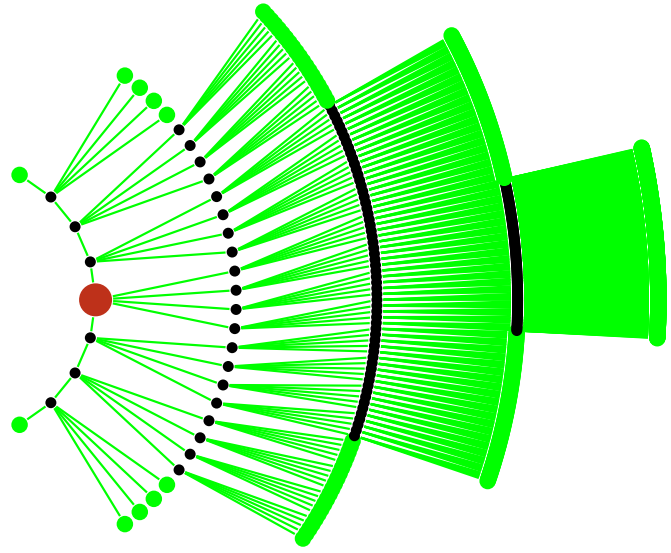


Isogeny-based cryptography (2)

Alice: 7



Bob: 5



State of SIDH / SIKE

(NIST level I security)

1. **SIKE** key encapsulation [Jao+]
   - $\sim$ 330-byte public keys / ciphertexts
   - $\sim$ 6.3 ms for enc + dec (constant-time)

   (Recall CSIDH has 64-byte pk and $\sim$ 246 ms exchange)

State of SIDH / SIKE

(NIST level I security)

1. **SIKE** key encapsulation [Jao+]
   - $\sim$ 330-byte public keys / ciphertexts
   - $\sim$ 6.3 ms for enc + dec (constant-time)

   (Recall CSIDH has 64-byte pk and $\sim$ 246 ms exchange)
2. Public-key compression [Aza+16; Cos+17; Zan+18; NR19]
   - $\sim$ 200-byte public keys / ciphertexts
   - $\sim$ 9.5 ms for enc + dec (constant-time)

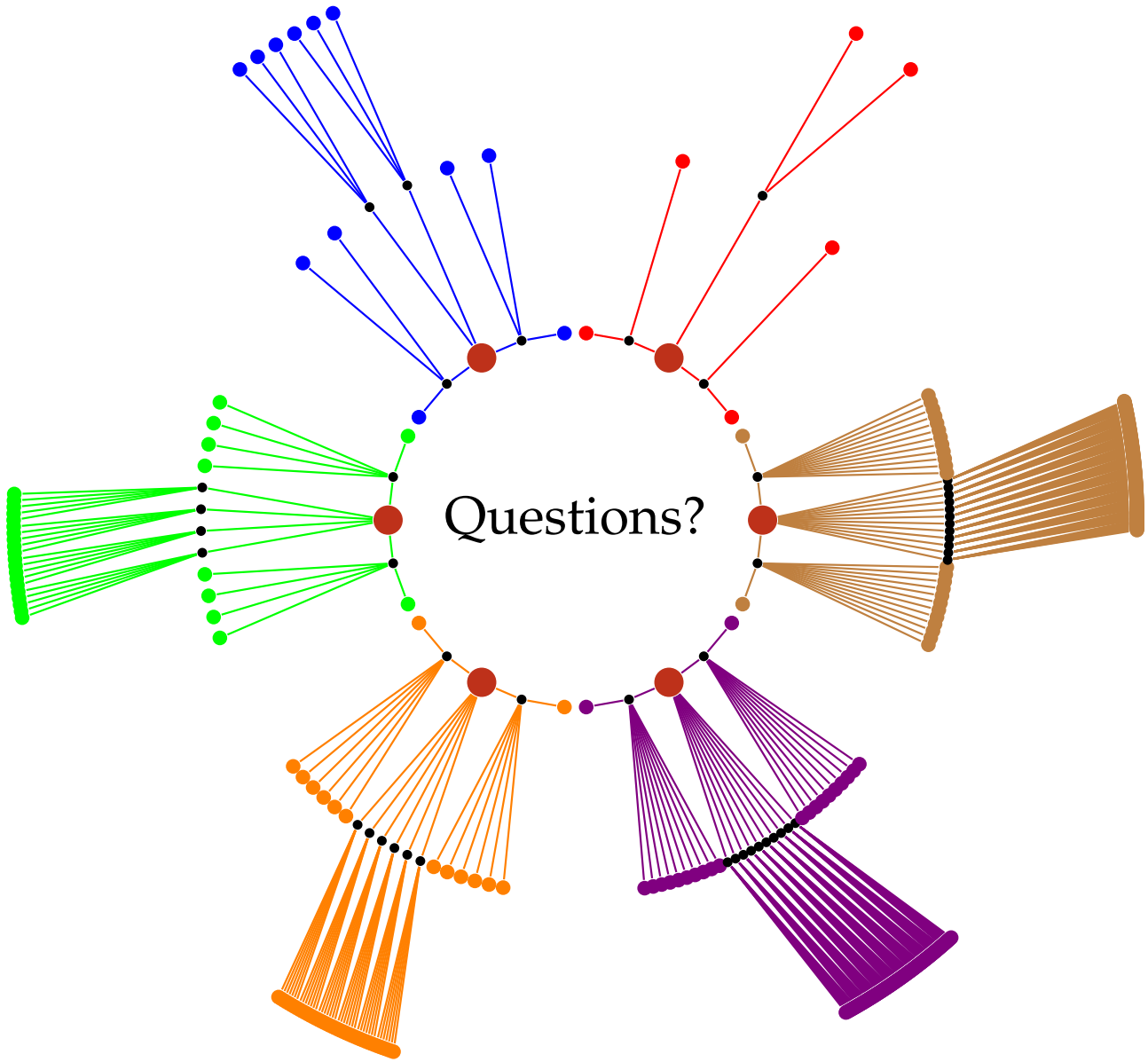
State of SIDH / SIKE

(NIST level I security)

1. **SIKE** key encapsulation [Jao+]
   - $\sim$ 330-byte public keys / ciphertexts
   - $\sim$ 6.3 ms for enc + dec (constant-time)

   (Recall CSIDH has 64-byte pk and $\sim$ 246 ms exchange)
2. Public-key compression [Aza+16; Cos+17; Zan+18; NR19]
   - $\sim$ 200-byte public keys / ciphertexts
   - $\sim$ 9.5 ms for enc + dec (constant-time)
3. Signatures *large* and *slow* [Yoo+17; GPS17]

Thanks!



References I

[Aza+16] Reza Azarderakhsh, David Jao, Kassem Kalach, Brian Koziel and Christopher Leonardi. 'Key Compression for Isogeny-Based Cryptosystems'. In: *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography, AsiaPKC@AsiaCCS, Xi'an, China, May 30 - June 03, 2016*. Ed. by Keita Emura, Goichiro Hanaoka and Rui Zhang. ACM, 2016, pp. 1–10. DOI: 10.1145/2898420.2898421. URL: http://doi.acm.org/10.1145/2898420.2898421.

[Ber+19] Daniel J. Bernstein, Tanja Lange, Chloe Martindale and Lorenz Panny. 'Quantum Circuits for the CSIDH: Optimizing Quantum Evaluation of Isogenies'. In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 409–441. ISBN: 978-3-030-17656-3. DOI: 10.1007/978-3-030-17656-3_15.

[BKV19] Ward Beullens, Thorsten Kleinjung and Frederik Vercauteren. *CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations*. Cryptology ePrint Archive, Report 2019/498. https://eprint.iacr.org/2019/498. 2019.

References II

[BS18] Xavier Bonnetain and André Schrottenloher. *Quantum Security Analysis of CSIDH and Ordinary Isogeny-based Schemes*. IACR Cryptology ePrint Archive 2018/537, version 20180621:135910. https://eprint.iacr.org/2018/537/20180621:135910. 2018.

[Cas+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny and Joost Renes. 'CSIDH: An Efficient Post-Quantum Commutative Group Action'. In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Cham: Springer International Publishing, 2018, pp. 395–427. ISBN: 978-3-030-03332-3.

[CLG09] Denis X. Charles, Kristin E. Lauter and Eyal Z. Goren. 'Cryptographic Hash Functions from Expander Graphs'. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 1432-1378. DOI: 10.1007/s00145-007-9002-x. URL: https://doi.org/10.1007/s00145-007-9002-x.

References III

[Cos+17] Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes and David Urbanik. 'Efficient Compression of SIDH Public Keys'. In: *Advances in Cryptology – EUROCRYPT 2017*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Cham: Springer International Publishing, 2017, pp. 679–706. ISBN: 978-3-319-56620-7.

[Cou06] Jean-Marc Couveignes. *Hard Homogeneous Spaces*. IACR Cryptology ePrint Archive 2006/291 `https://ia.cr/2006/291`. 2006.

[DG19] Luca De Feo and Steven D. Galbraith. 'SeaSign: Compact Isogeny Signatures from Class Group Actions'. In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 759–789. ISBN: 978-3-030-17659-4. DOI: 10.1007/978-3-030-17659-4_26.

References IV

[DKS18] Luca De Feo, Jean Kieffer and Benjamin Smith. 'Towards Practical Key Exchange from Ordinary Isogeny Graphs'. In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by Thomas Peyrin and Steven Galbraith. Cham: Springer International Publishing, 2018, pp. 365–394. ISBN: 978-3-030-03332-3. DOI: 10.1007/978-3-030-03332-3_14.

[GPS17] Steven D. Galbraith, Christophe Petit and Javier Silva. 'Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems'. In: *Advances in Cryptology – ASIACRYPT 2017*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Cham: Springer International Publishing, 2017, pp. 3–33. ISBN: 978-3-319-70694-8. DOI: 10.1007/978-3-319-70694-8_1.

[Jao+] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev and David Urbanik. *SIKE. Supersingular Isogeny Key Encapsulation*. Submission to [**nistpqc**]. http://sike.org.

References V

[JF11] David Jao and Luca De Feo. 'Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies'. In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings*. 2011, pp. 19–34. DOI: 10.1007/978-3-642-25405-5_2. URL: http://dx.doi.org/10.1007/978-3-642-25405-5_2.

[Kob87] Neal Koblitz. 'Elliptic curve cryptosystems'. In: *Mathematics of Computation* 48 (1987), pp. 203–209. DOI: 10.1090/S0025-5718-1987-0866109-5.

[MCR18] Michael Meyer, Fabio Campos and Steffen Reith. *On Lions and Elligators: An efficient constant-time implementation of CSIDH*. Cryptology ePrint Archive, Report 2018/1198. https://eprint.iacr.org/2018/1198. 2018.

[Mil86] Victor S. Miller. 'Use of Elliptic Curves in Cryptography'. In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1. DOI: 10.1007/3-540-39799-X_31.

References VI

[NR19] Michael Naehrig and Joost Renes. *Dual Isogenies and Their Application to Public-key Compression for Isogeny-based Cryptography*. Cryptology ePrint Archive, Report 2019/499. https://eprint.iacr.org/2019/499. 2019.

[RS06] Alexander Rostovtsev and Anton Stolbunov. *Public-Key Cryptosystem Based on Isogenies*. IACR Cryptology ePrint Archive 2006/145 https://ia.cr/2006/145. 2006.

[Yoo+17] Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao and Vladimir Soukharev. 'A Post-Quantum Digital Signature Scheme Based on Supersingular Isogenies'. In: *IACR Cryptology ePrint Archive* 2017 (2017), p. 186. URL: http://eprint.iacr.org/2017/186.

References VII

[Zan+18] Gustavo H. M. Zanon, Marcos A. Simplicio, Geovandro C. C. F. Pereira, Javad Doliskani and Paulo S. L. M. Barreto. 'Faster Isogeny-Based Compressed Key Agreement'. In: *Post-Quantum Cryptography*. Ed. by Tanja Lange and Rainer Steinwandt. Cham: Springer International Publishing, 2018, pp. 248–268. ISBN: 978-3-319-79063-3. DOI: 10.1007/978-3-319-79063-3_12.